industrial internet CONSORTIUM

Industrial Internet of Things Security Framework

October 2016

Approved for Public Release; Distribution Unlimited. Case Number 16-0696

Industrial Internet Consortium

Mission

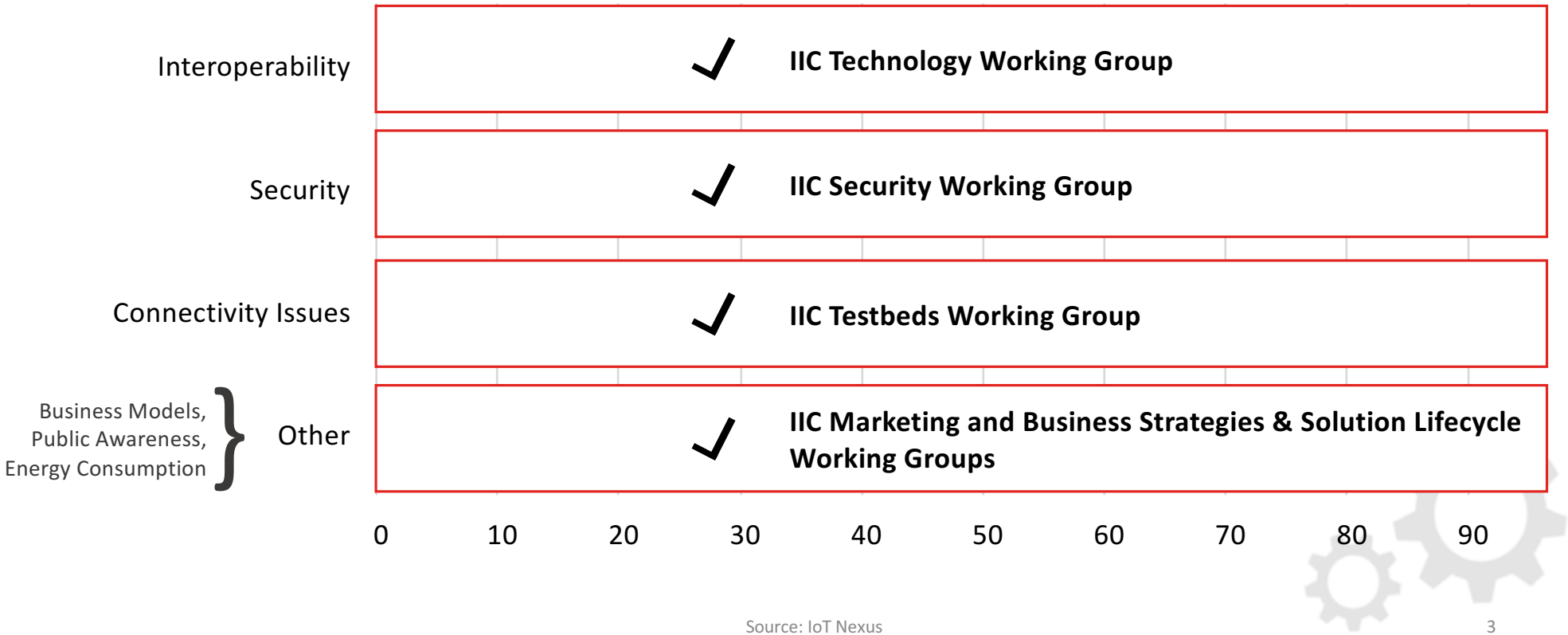
To **accelerate growth** of the Industrial Internet by **coordinating ecosystem** initiatives to connect and integrate objects with **people, processes and data** using common architectures, interoperability and open standards that lead to **transformational business outcomes**.

Launched in March 2014 – now over 250 members

250+ Member Organizations
Spanning 28 Countries

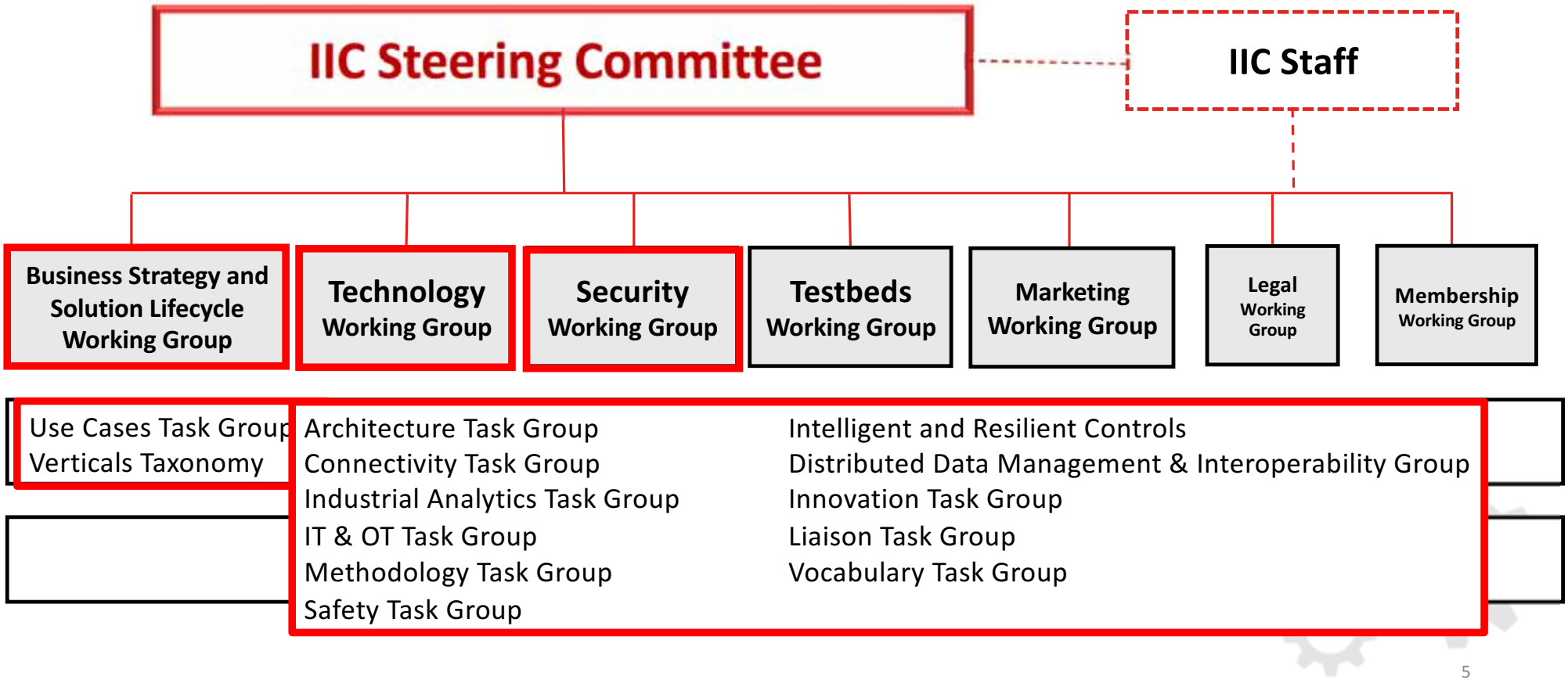
The IIC is an open, neutral "sandbox" where industry, academia and government meet to collaborate, innovate and enable.

What is the Biggest Challenge Facing the Industrial Internet?



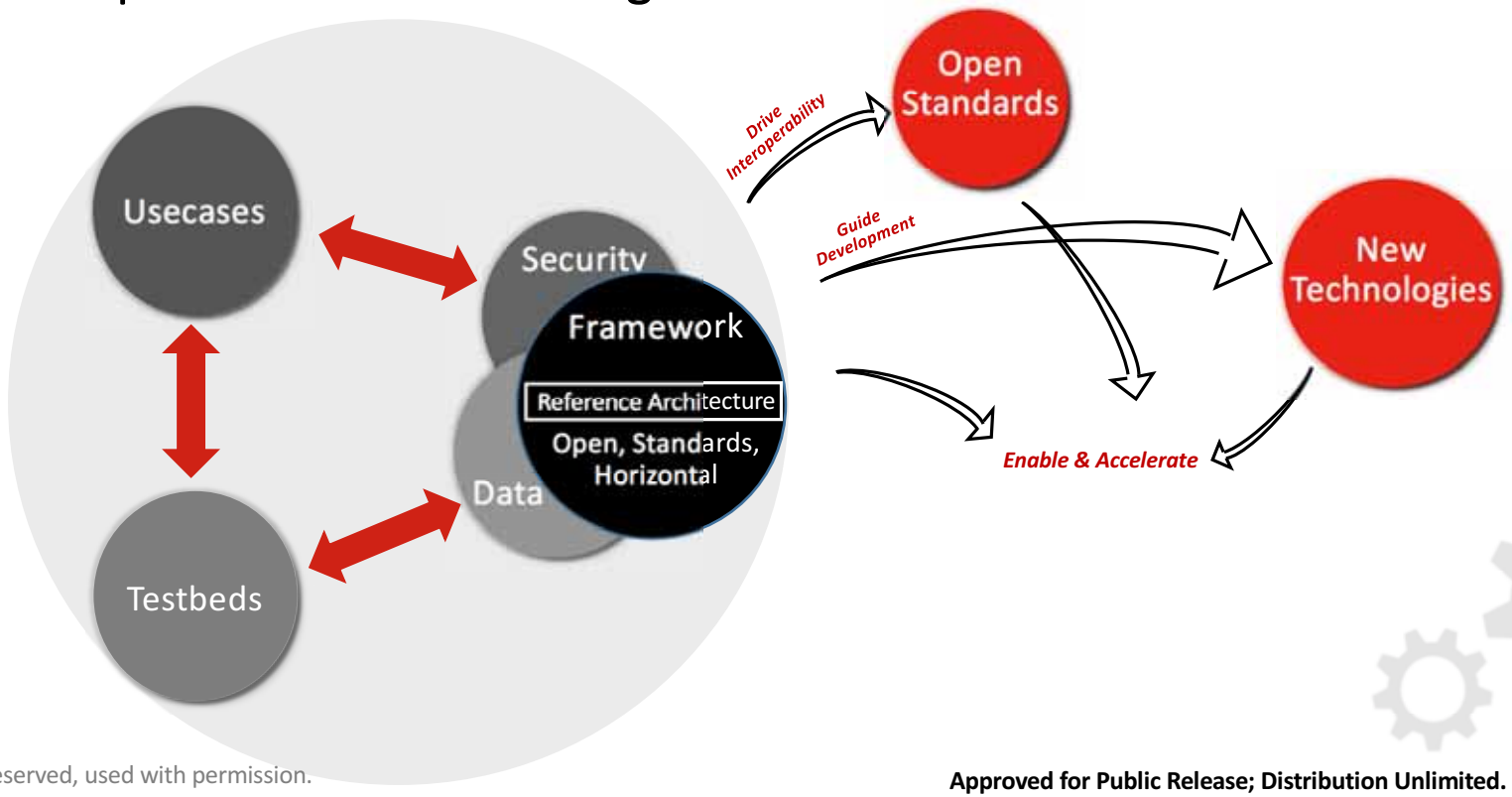
Source: IoT Nexus

How the IIC efforts are Organized



Collaboration within the Industrial Internet Consortium

IIC Working Groups have individual charters, inter-related outcomes both within the Working Groups and with external organizations.



Industrial Internet Consortium Testbeds:

http://www.iiconsortium.org/wc-testbeds.htm

The IIC and Standards Organizations

The IIC is *not* a standards organization.

It evaluates and organizes existing standards to:

- Advocate for open standard technologies
- Influence the global standards development

The Technology Working Group is currently:

- Evaluating existing standards
- Identifying requirements for the Industrial Internet

IIC Formal Liaisons as of July 2016

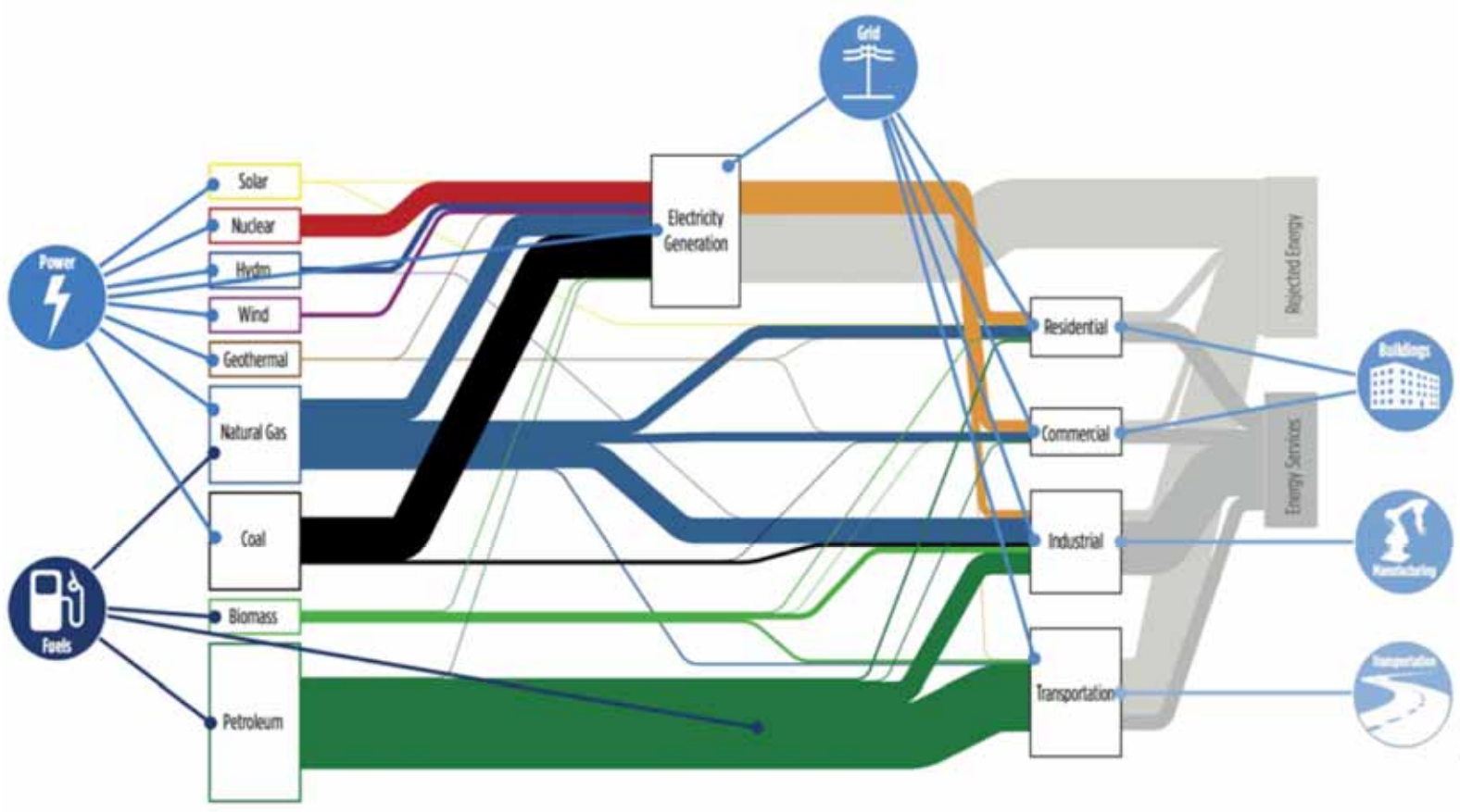
Industrial Internet Reference Architecture

- **<u>110-page document published and released to public June 2015</u>**

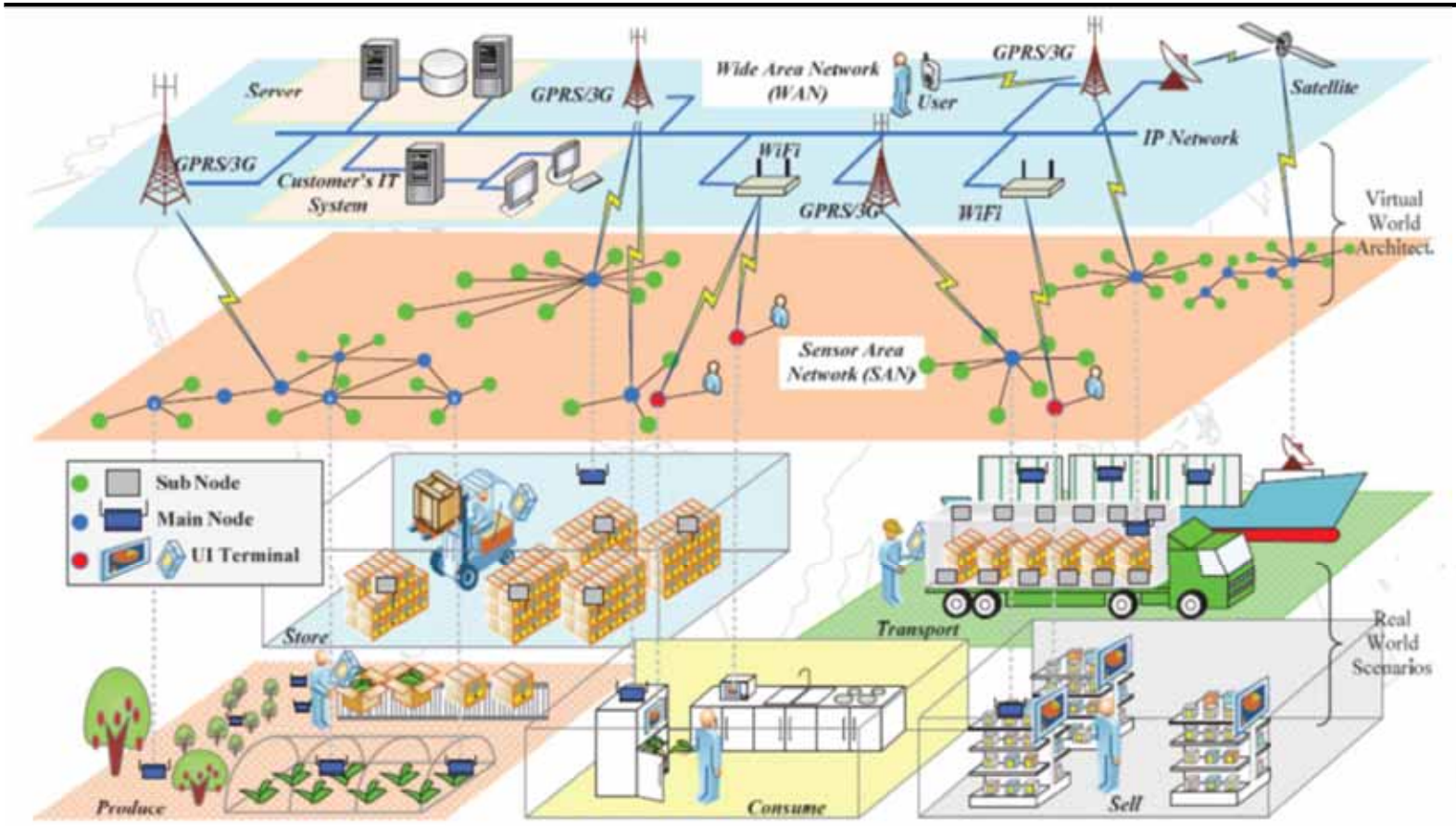
- **Goal:** To align the industry to a common end-to-end Industrial IoT reference architecture with clearly defined constituent components and interfaces between them so that:
  - Vendors can deliver interchangeable IoT components that are interoperative with those provided by other venders;
  - Customers can use the reference architecture as a blueprint, based on which to build and/or select technologies and solutions from venders for their IoT implementation.
- **Requirements addressed:**
  - Concise and comprehensive description of the end-to-end IoT architecture for the industrial internet industry space
  - Clear definition of constituent components and interfaces between the components
  - High-level functional requirements for each of the components
  - Identification of existing or to be developed technologies for these components
  - Inspired and validated by core use cases
  - Implemented and tested in an IIC testbed

The IIRA Addresses Complexities in: Ecosystems

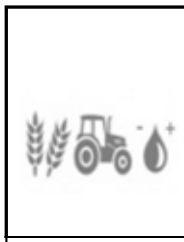
The IIRA Addresses Complexities in: Sector-2-Sector Linkages



The IIRA Addresses Complexities in: Networks

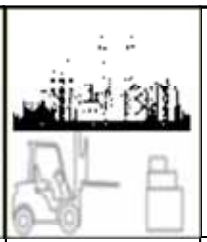


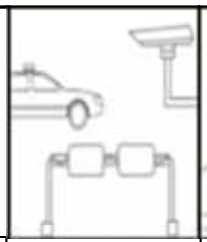
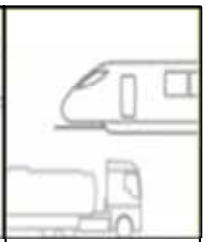
The IIRA Addresses Complexities in: Sectors & Verticals





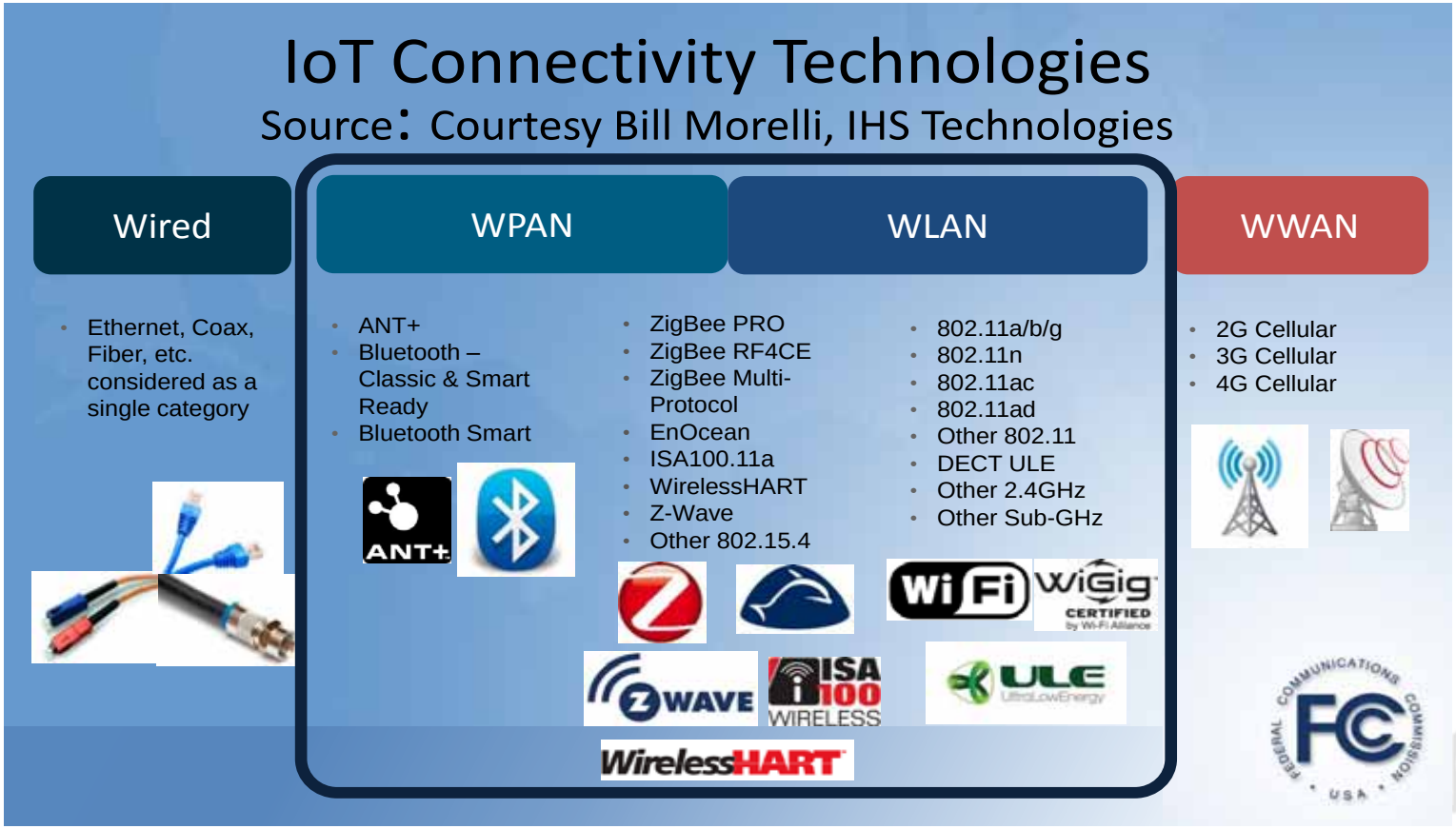




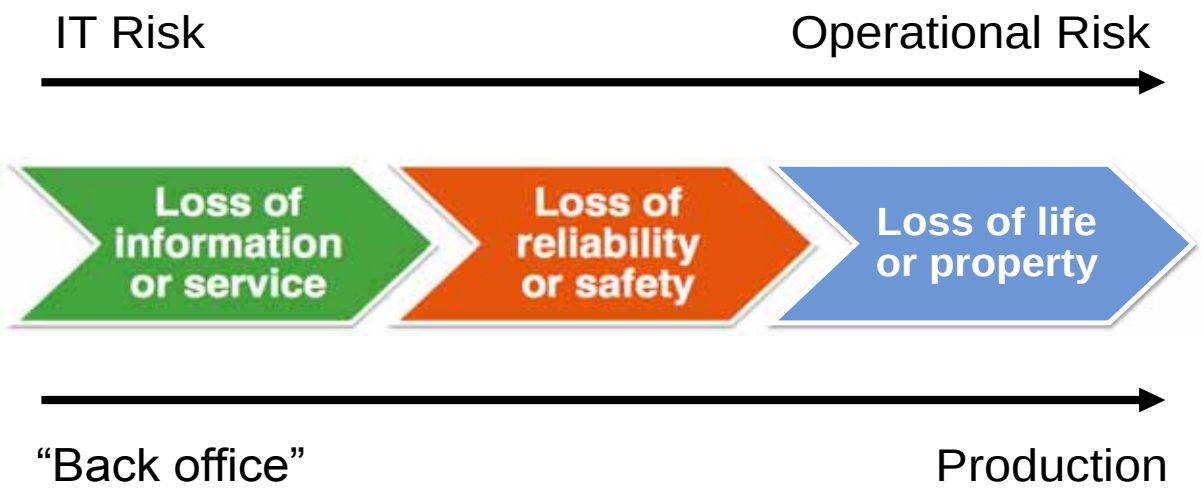



agriculture	building	consumer & home	defense/ aerospace	energy	healthcare	manufacturing	public sector	public security & safety	transportation
farming, ranching, fishing, weather	*building/ construction, smart home, office, building security, building maintenance*	*consumer products, home products, cooking (commercial), entertainment, phone & network services, sporting events, travel, tourism*	*defense, military, aerospace*	*energy, utilities, mining, oil and gas, smart grid*	*connected medical devices, hospitals, medical offices, pharmacies, medical therapy, home healthcare, disease diagnosis, continuous patient monitoring, clinical trials, assisted care, dentistry*	*factory, industrial automation, smart products*	*education, environment, water, transportation, waste management, civil administration*	*public safety, public security, surveillance, disaster prevention. Law enforcement/ police, fire, emergency and crisis response, and military*	*mobility, transportation, public transportation, vehicle, traffic infrastructure, logistics, freight management, pipelines, shipping, aeronautics*

The IIRA Addresses Complexities in: Sets of Connectivity Options

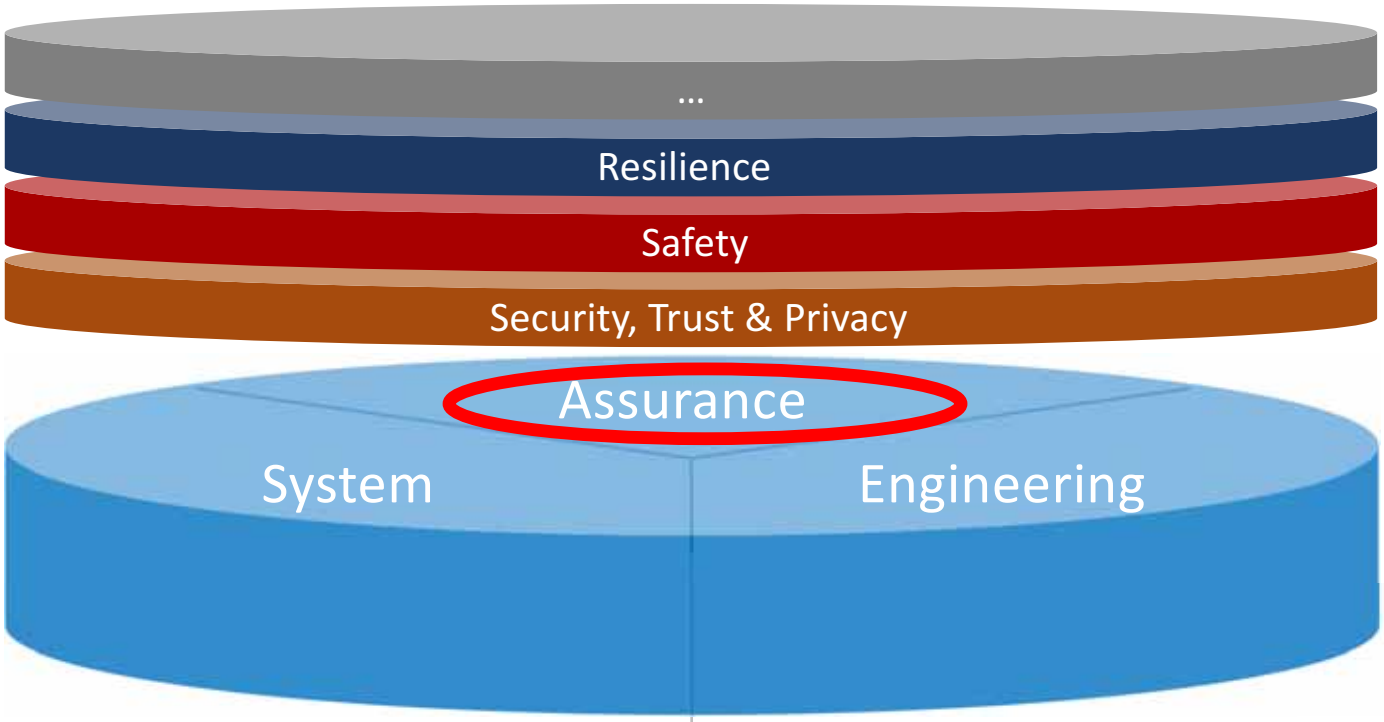


Cyber Risk is Expanding into Physical Risk



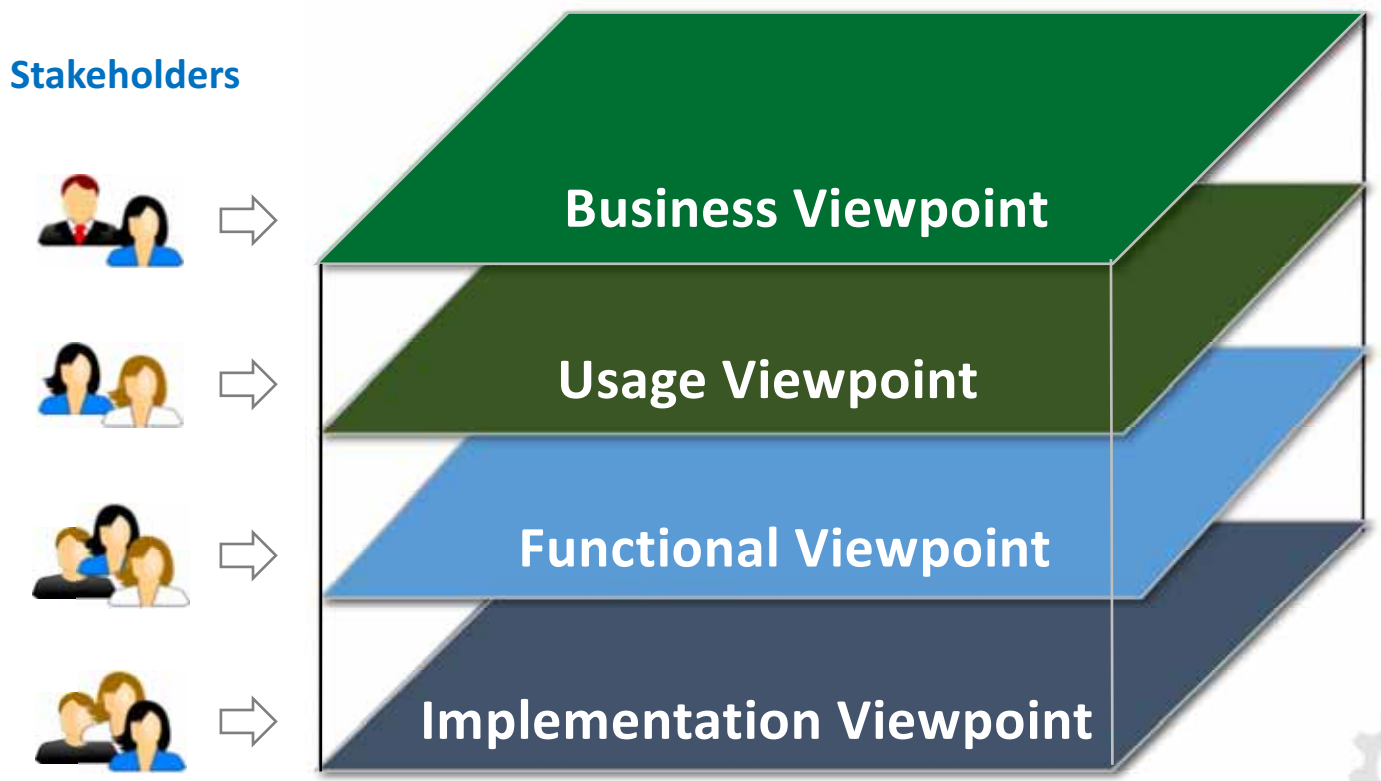
Gartner

Key System Characteristics and their Assurance – Chapter 2



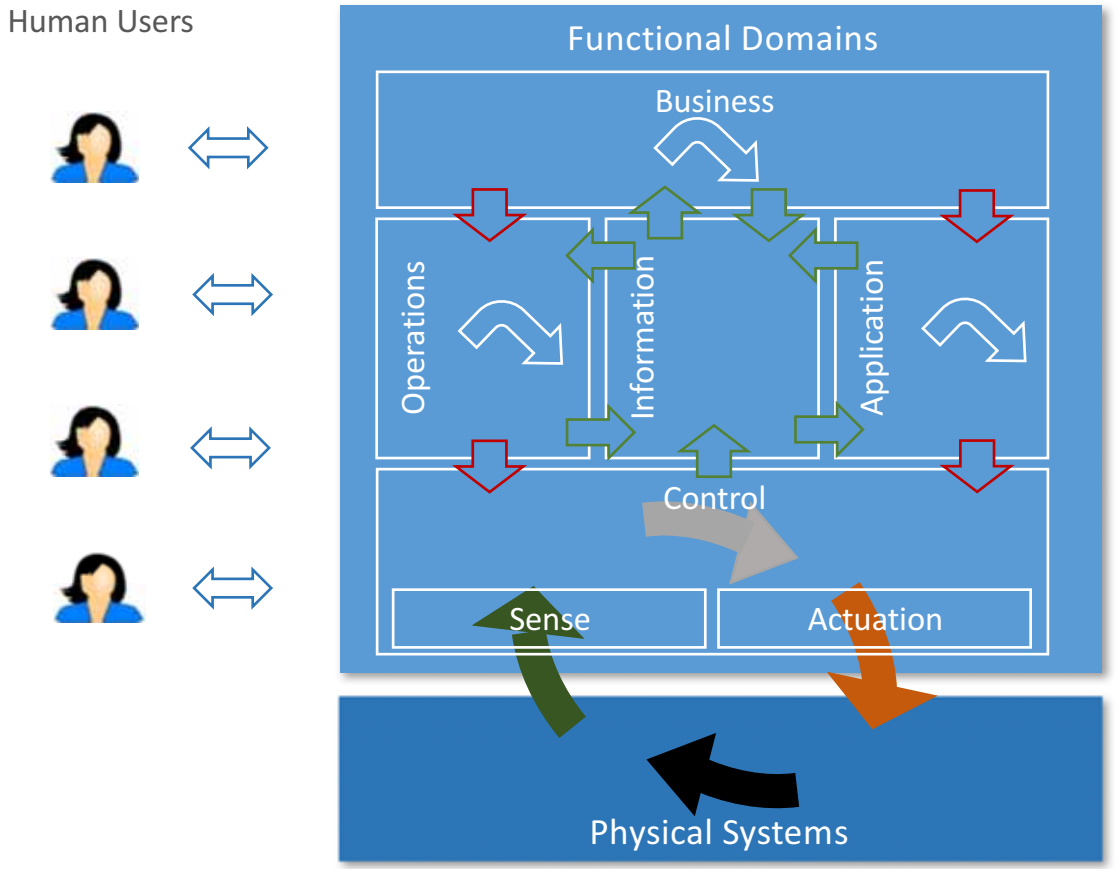
- **ISO Assurance Case Standard**
- **OMG Structured Assurance Case Metamodel Standard**
- **Open Group Dependability through Assurance Standard**

Industrial Internet Reference Architecture – Chapters 3, 4, 5, 6, & 7



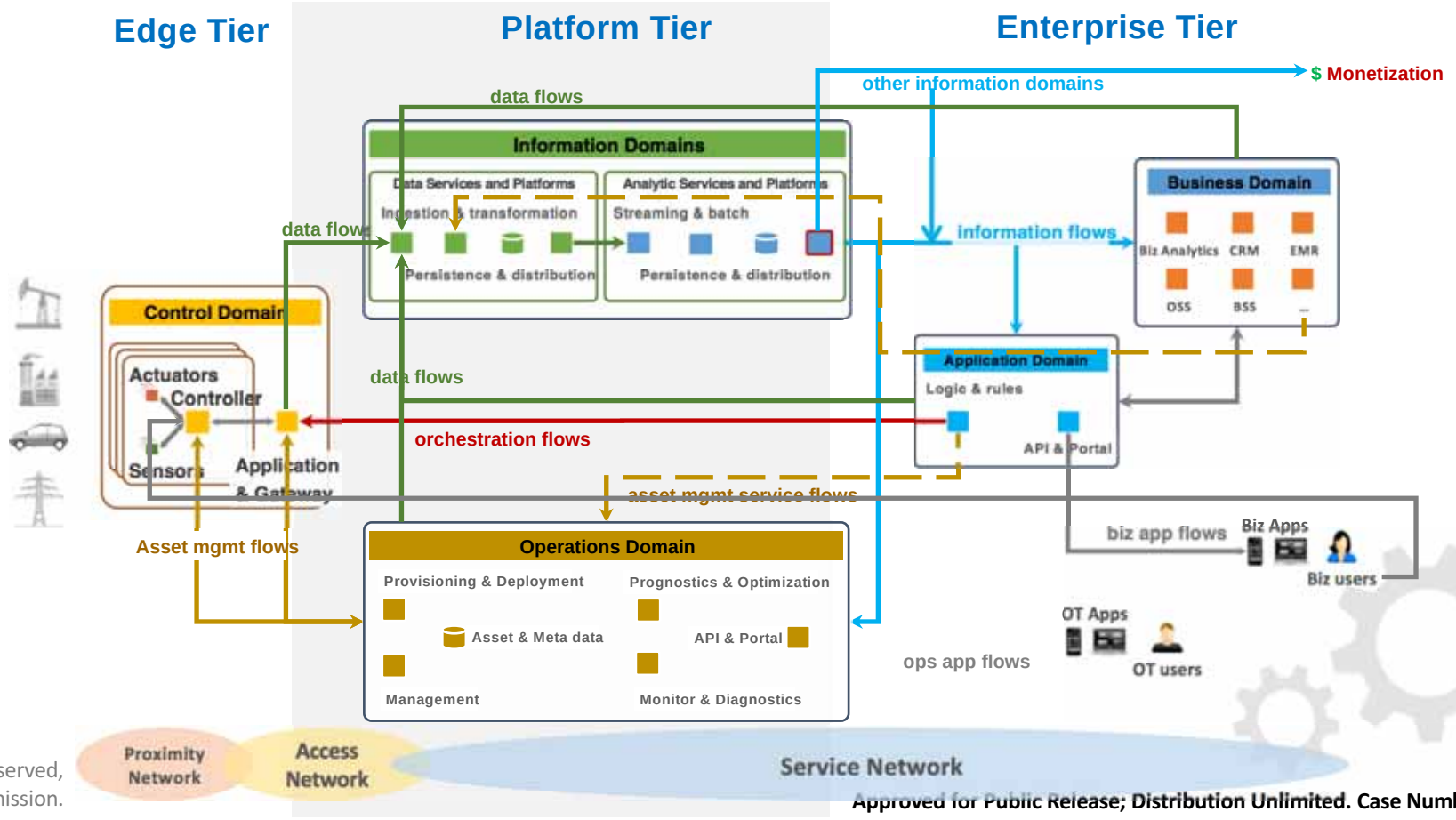
Viewpoints – Chapter 6 – Functional Viewpoint

IIRA Functional View



Viewpoints – Chapter 7 – Implementation Viewpoint

IIoT System View



Industrial Internet of Things (IIoT) Security Framework (September 19, 2016)

http://www.iiconsortium.org/IISF.htm

Industrial Internet of Things
Volume G4: Security Framework

IIC:PUB:G4:V1.0:PB:20160926

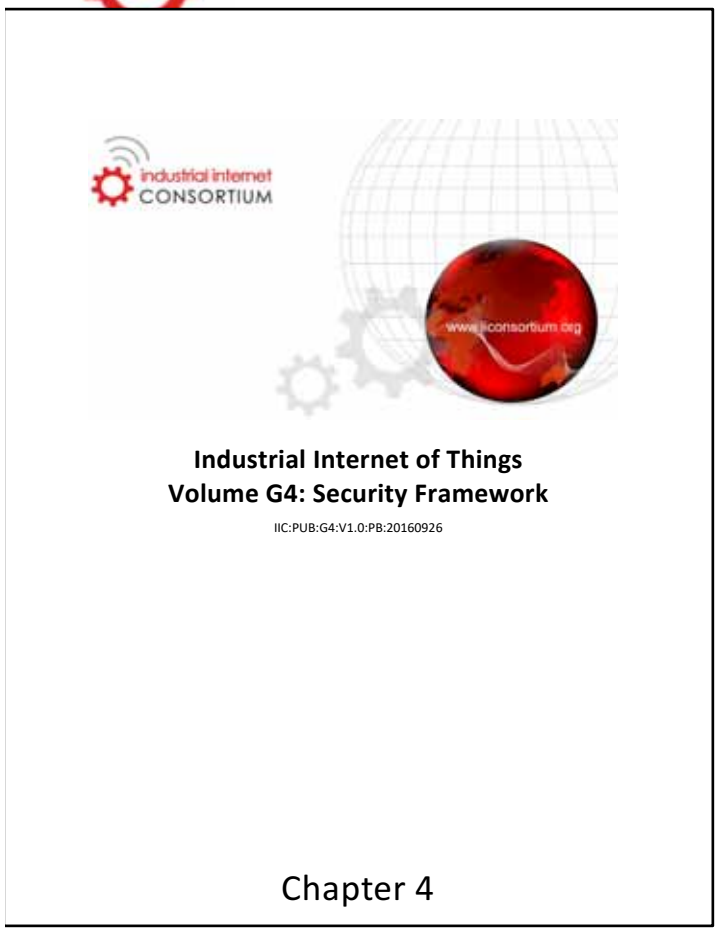
PRIMARY AUTHORS:

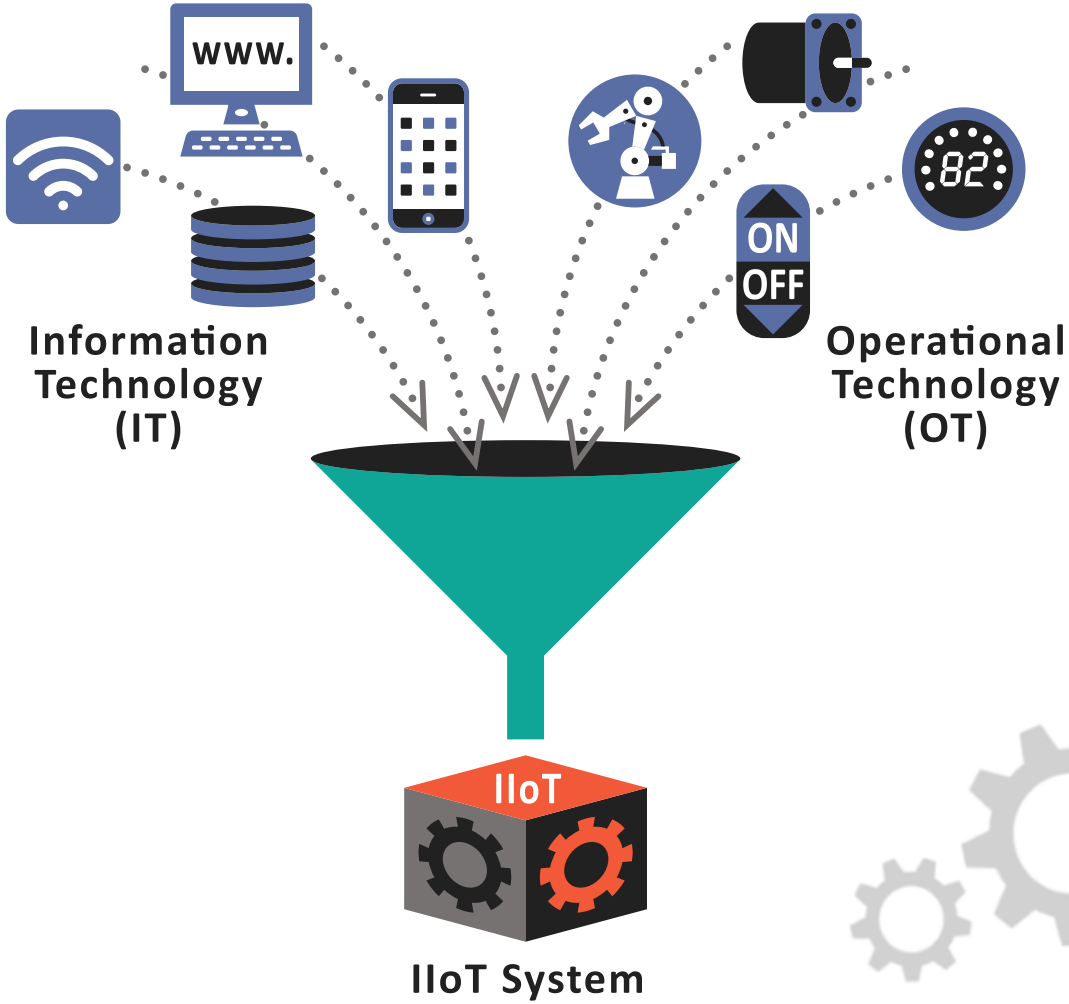
- Sven Schrecker - Intel Corporation
- Hamed Soroush - Real-Time Innovations
- Jesus Molina - Fujitsu Limited
- Marcellus Buchheit - Wibu-Systems
- JP LeBlanc - Lynx Software Technologies
- Robert Martin - The MITRE Corporation
- Frederick Hirsch - Fujitsu Limited
- Andrew Ginter - Waterfall Security Solutions
- Harsha Banavara - Schneider Electric
- Shrinath Eswarahally - Infineon Technologies
- Kaveri Raman - AT&T
- Andrew King - University of Pennsylvania
- Qinqing (Christine) Zhang - Johns Hopkins University
- Peter MacKay - GE Wurldtech
- Brian Witten - Symantec

OTHER CONTRIBUTORS:

- AO Kaspersky Lab
- Belden
- Bosch
- Cisco
- CyberX
- EMC
- ENT Technologies
- General Electric
- GlobalSign
- Hitachi
- Huawei
- IBM
- Microsoft
- Oracle
- Tata Consultancy Services
- Thingswise
- Toshiba

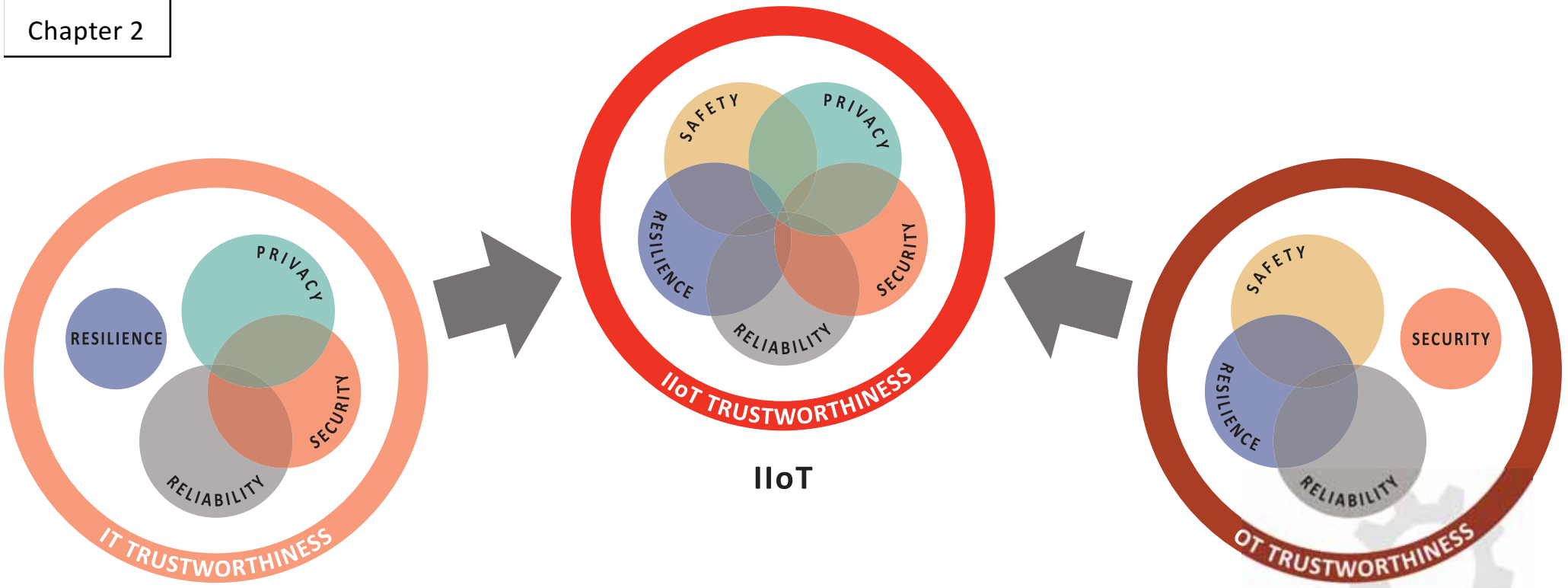
Convergence of Information Technology and Operational Technology





Chapter 2

CONVERGENCE OF IT AND OT TRUSTWORTHINESS

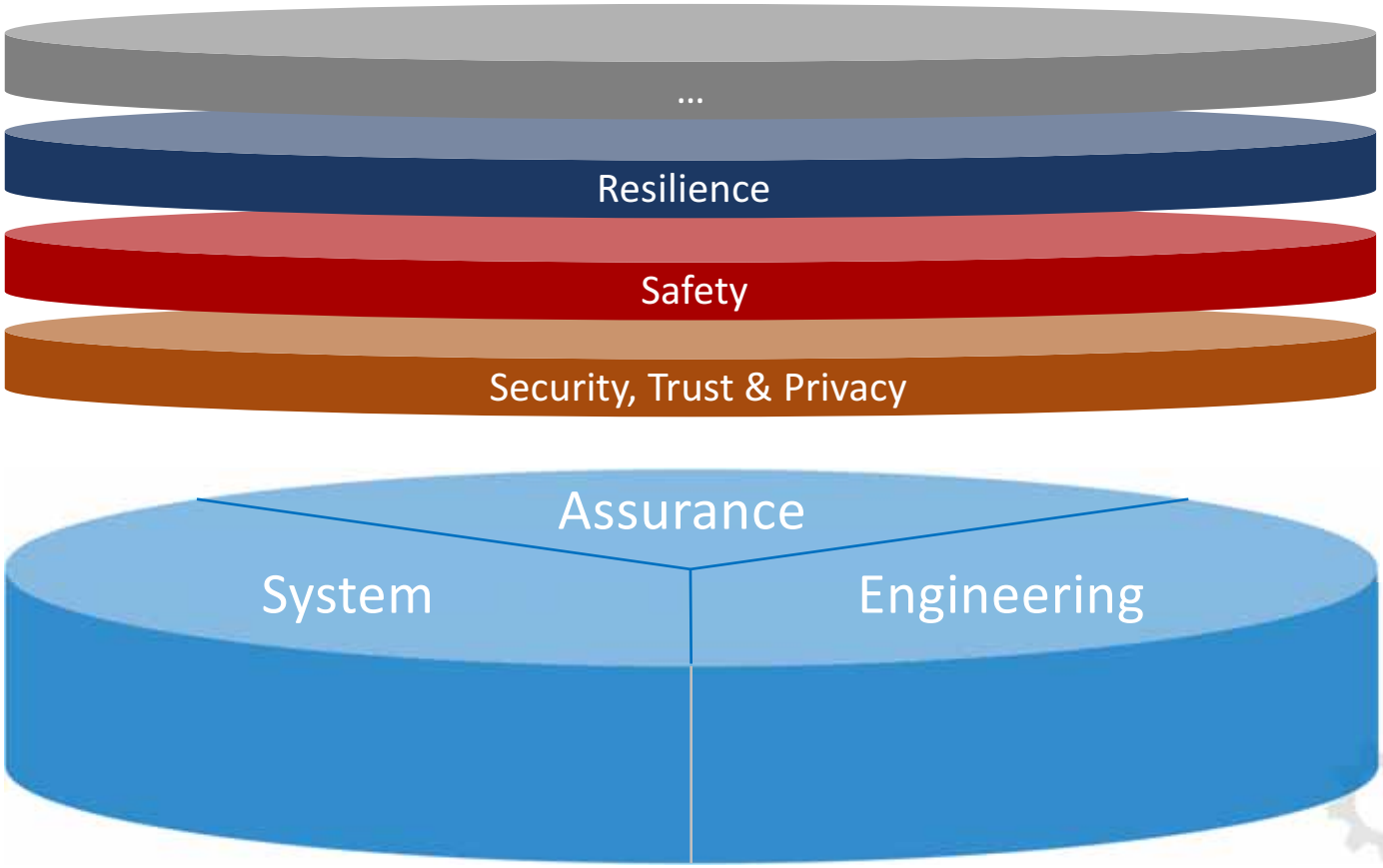


Information Technology (IT)

IIoT

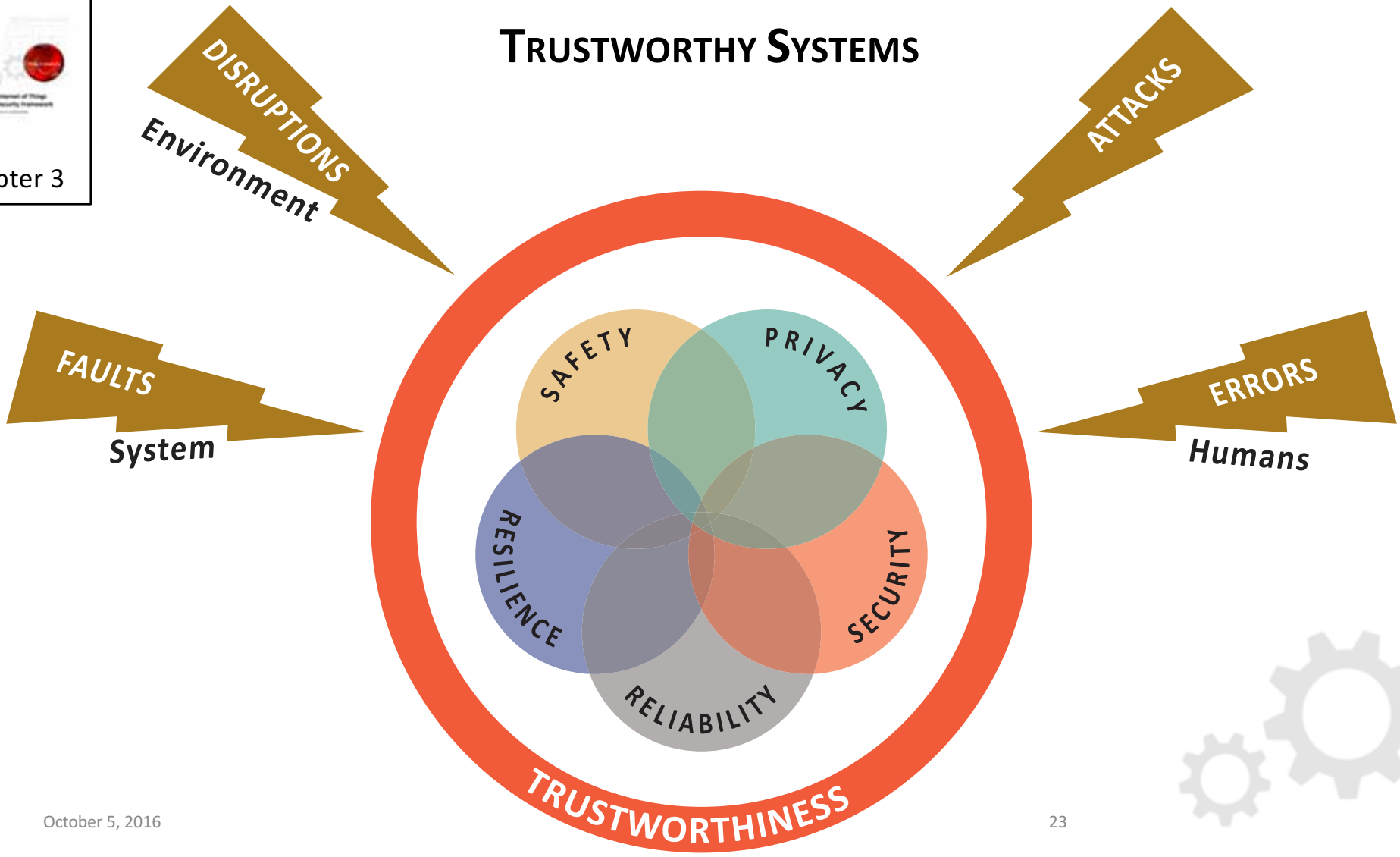
Operational Technology (OT)

Key System Characteristics and their Assurance – Chapter 2



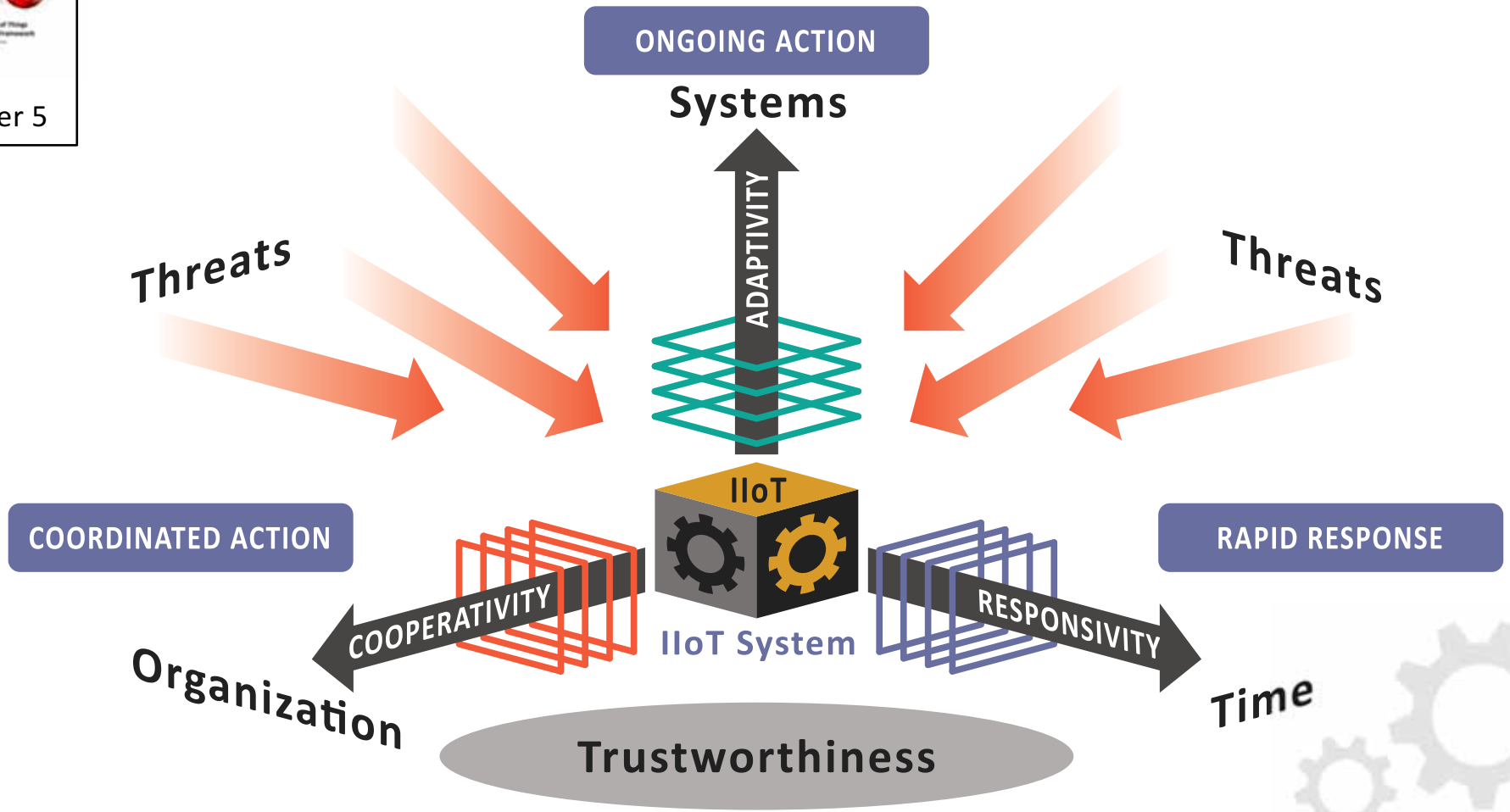
Chapter 3

TRUSTWORTHY SYSTEMS



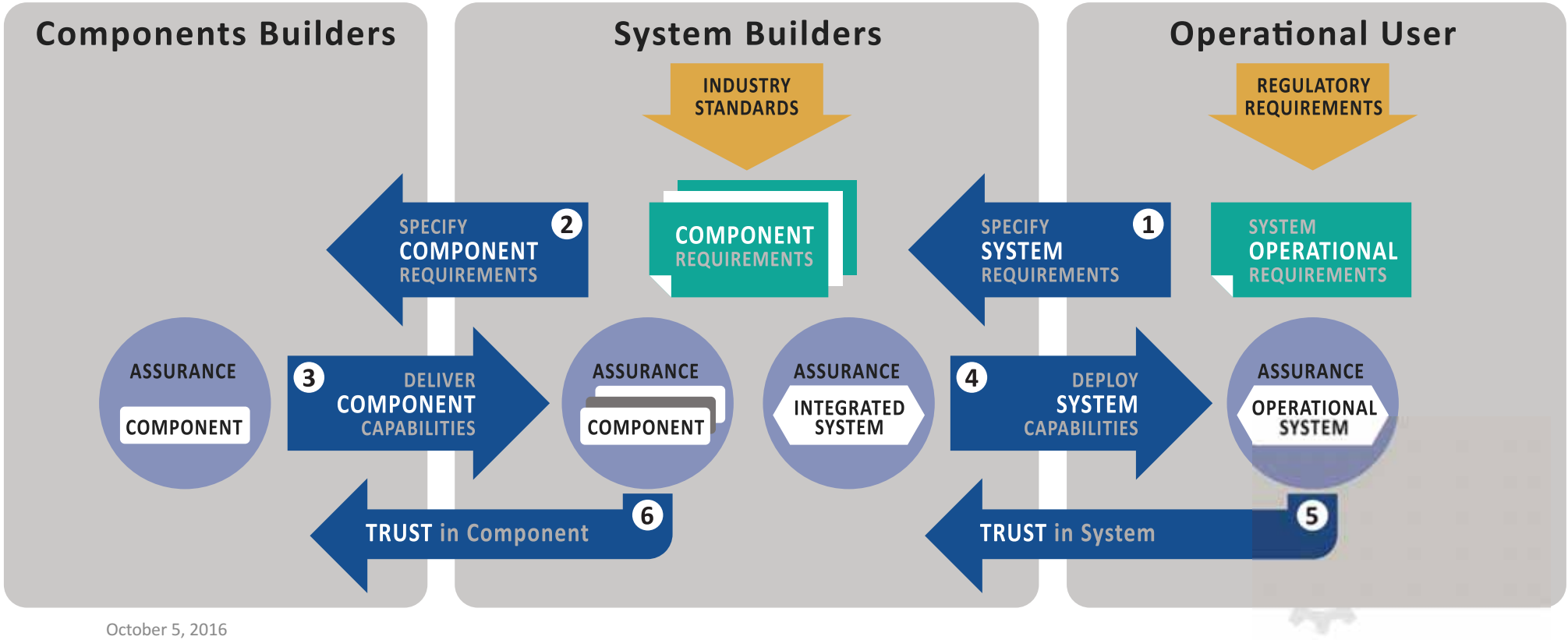
Chapter 5

TRUSTWORTHINESS MANAGEMENT CONSIDERATIONS



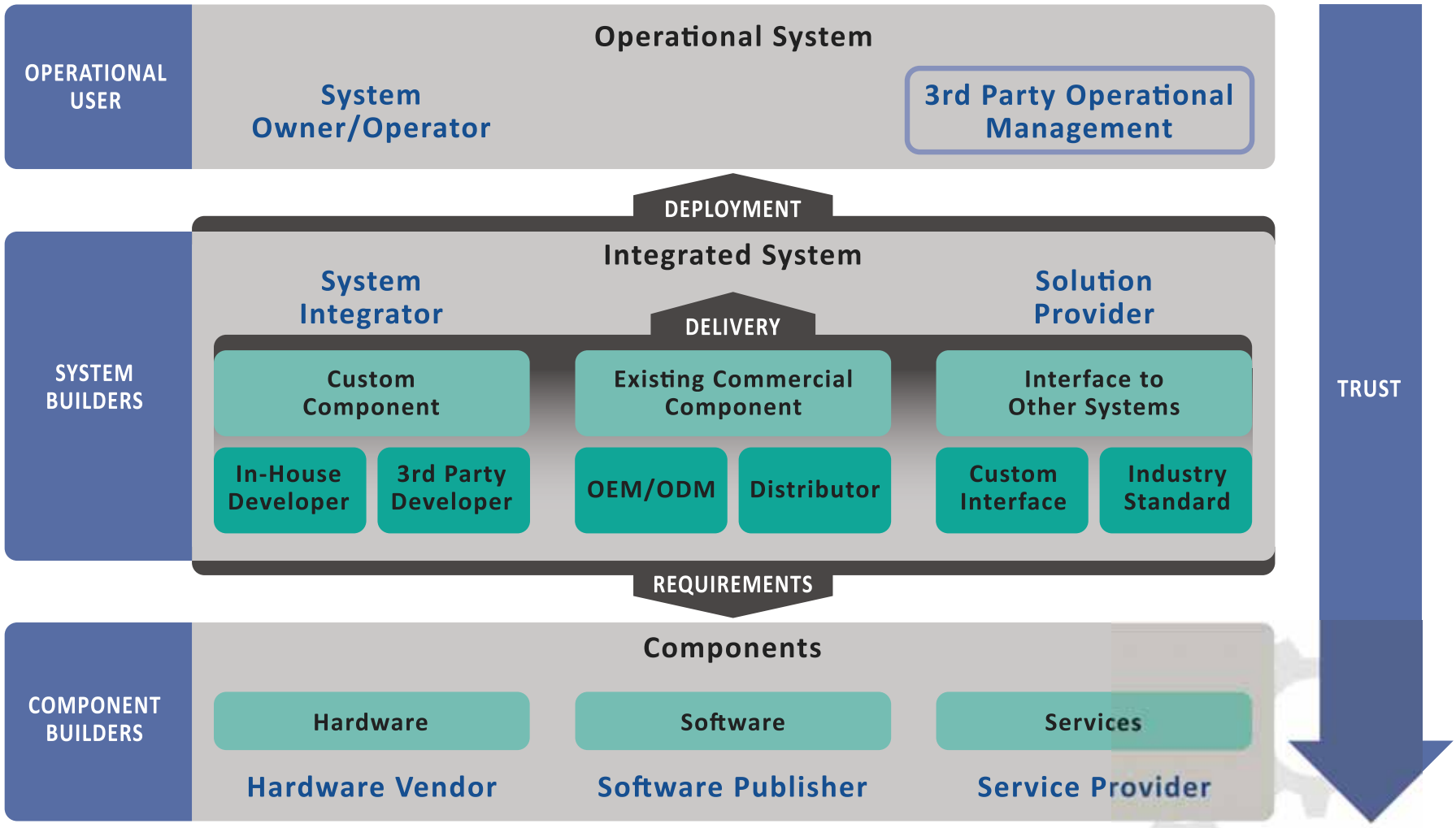
Chapter 6

PERMEATION OF TRUST



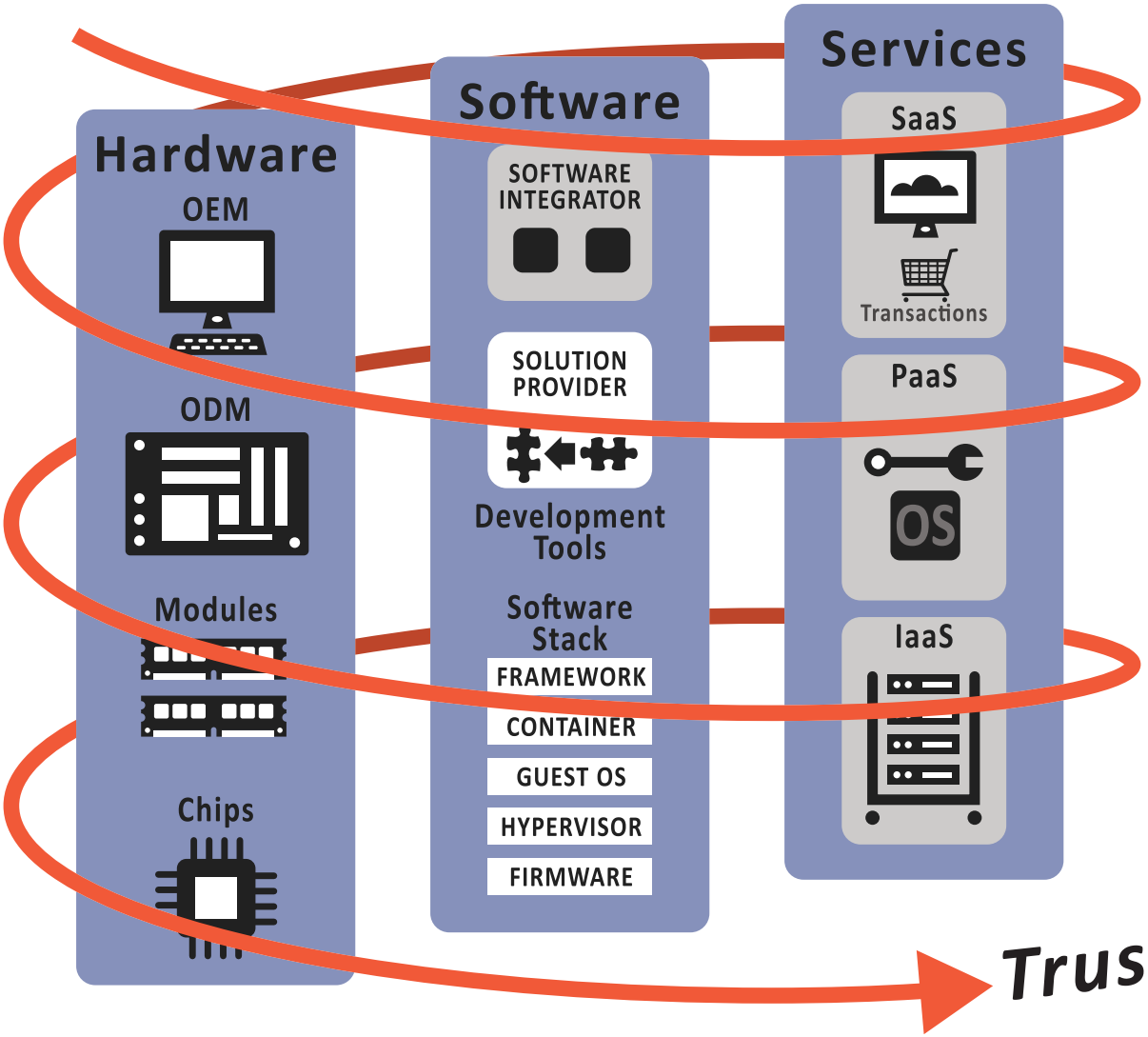
Chapter 6

TRUST RELATIONSHIP BETWEEN ACTORS



Chapter 6

TRUST RELATIONSHIP BETWEEN COMPONENT BUILDERS



Chapter 7

IISF FUNCTIONAL VIEWPOINT - SECURITY BUILDING BLOCKS

Security Configuration & Management

Security Monitoring & Analysis

Communications & Connectivity Protection

Endpoint Protection

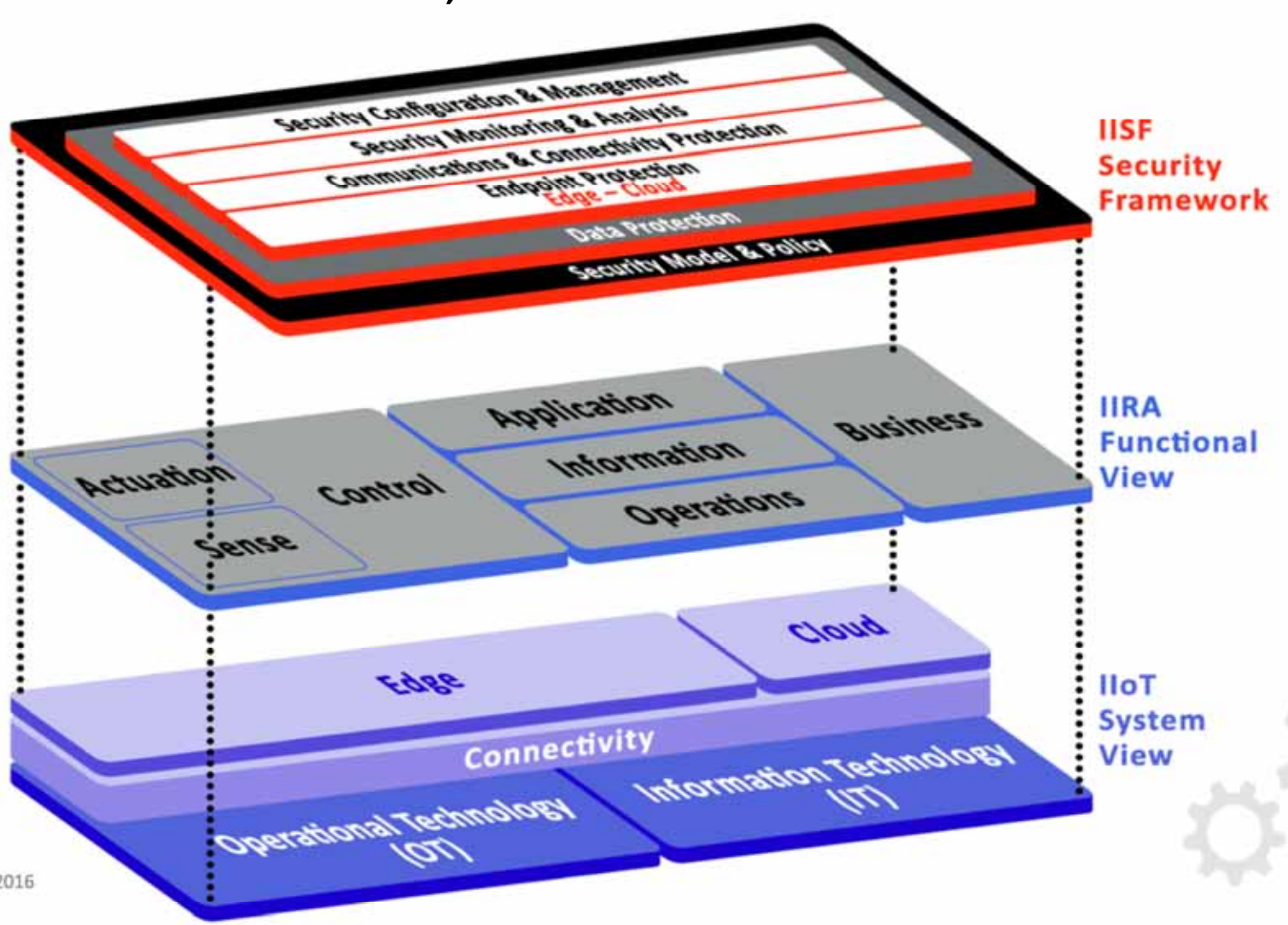
Edge – Cloud

Data Protection

Security Model & Policy

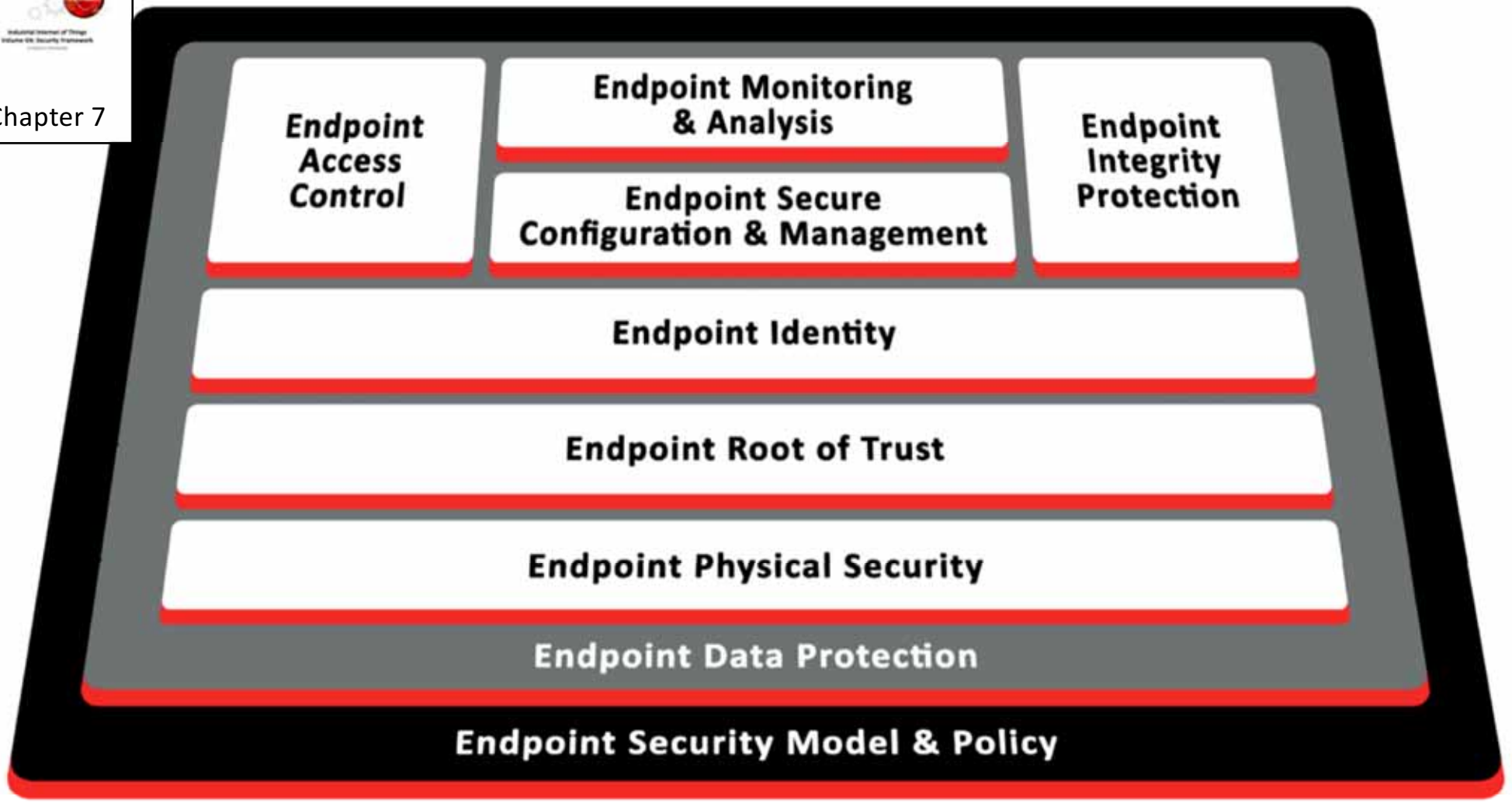
Chapter 7

ALIGNMENT OF IISF, IIRA FUNCTIONAL AND IIOT SYSTEM VIEWS



Chapter 7

Endpoint Protection



Chapter 7

Communications & Connectivity Protection
Information Flow Protection
Network Configuration & Management
Network Monitoring & Analysis
Cryptographic Protection
Communicating Endpoints Protection
Physical Security of Connections
Data-in-Motion Protection
Security Policies for Communications & Connectivity Protection

Chapter 7

Security Monitoring & Analysis

Monitor	Analyze	Act
Endpoints & Communication	Behavioral Analysis	Proactive/ Predictive
Secure Remote Logging	Rule-Based Analysis	Reactive Detection & Recovery
Supply Chain		Root Cause/ Forensics

Monitoring & Analysis Data Protection

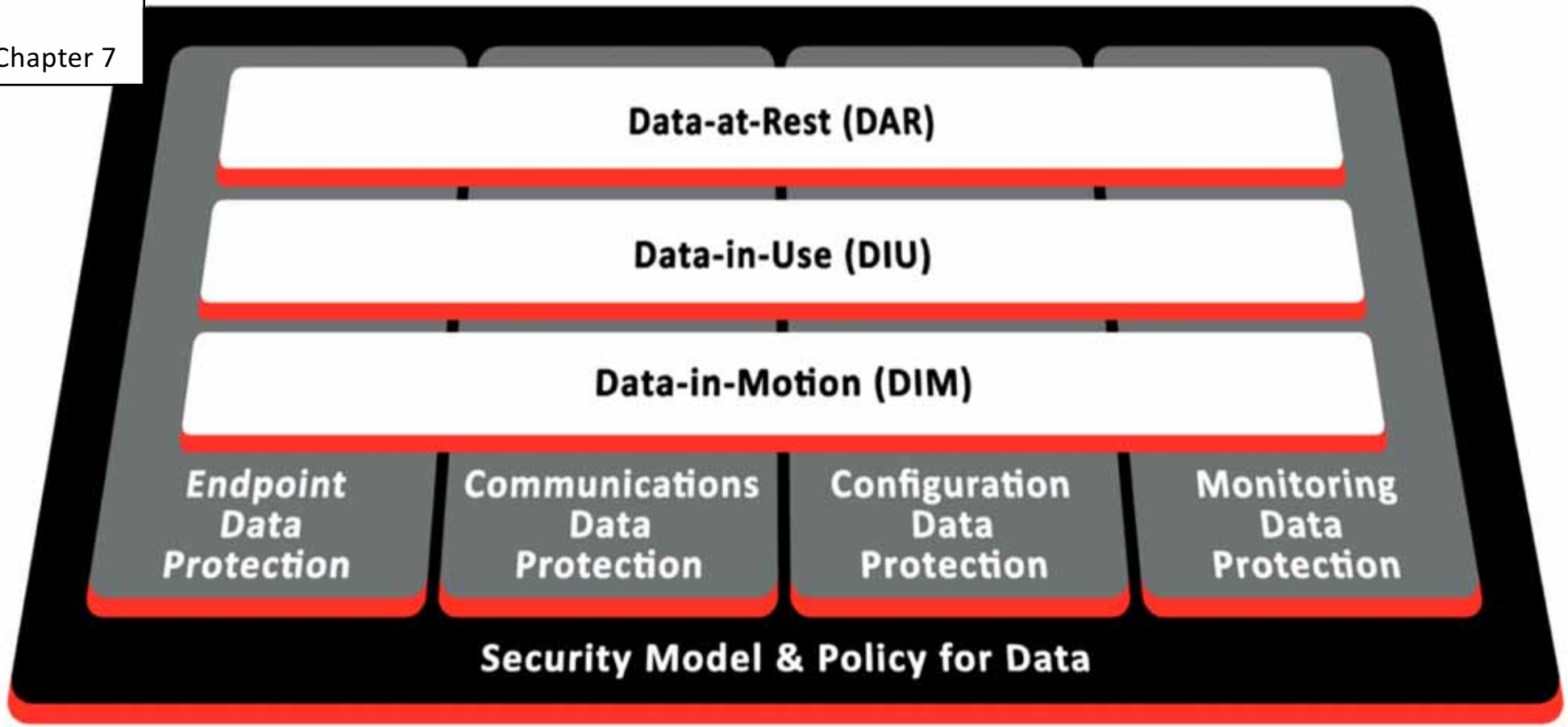
Security Model & Policy for Monitoring

Chapter 7

Security Configuration & Management
Secure Operational Management
Endpoint Identity Management
Endpoint Configuration & Management
Communications Configuration & Management
Security Management
Security Model Change Control
Configuration & Management Data Protection
Security Model & Policy for Change Management

Chapter 7

Protecting Data



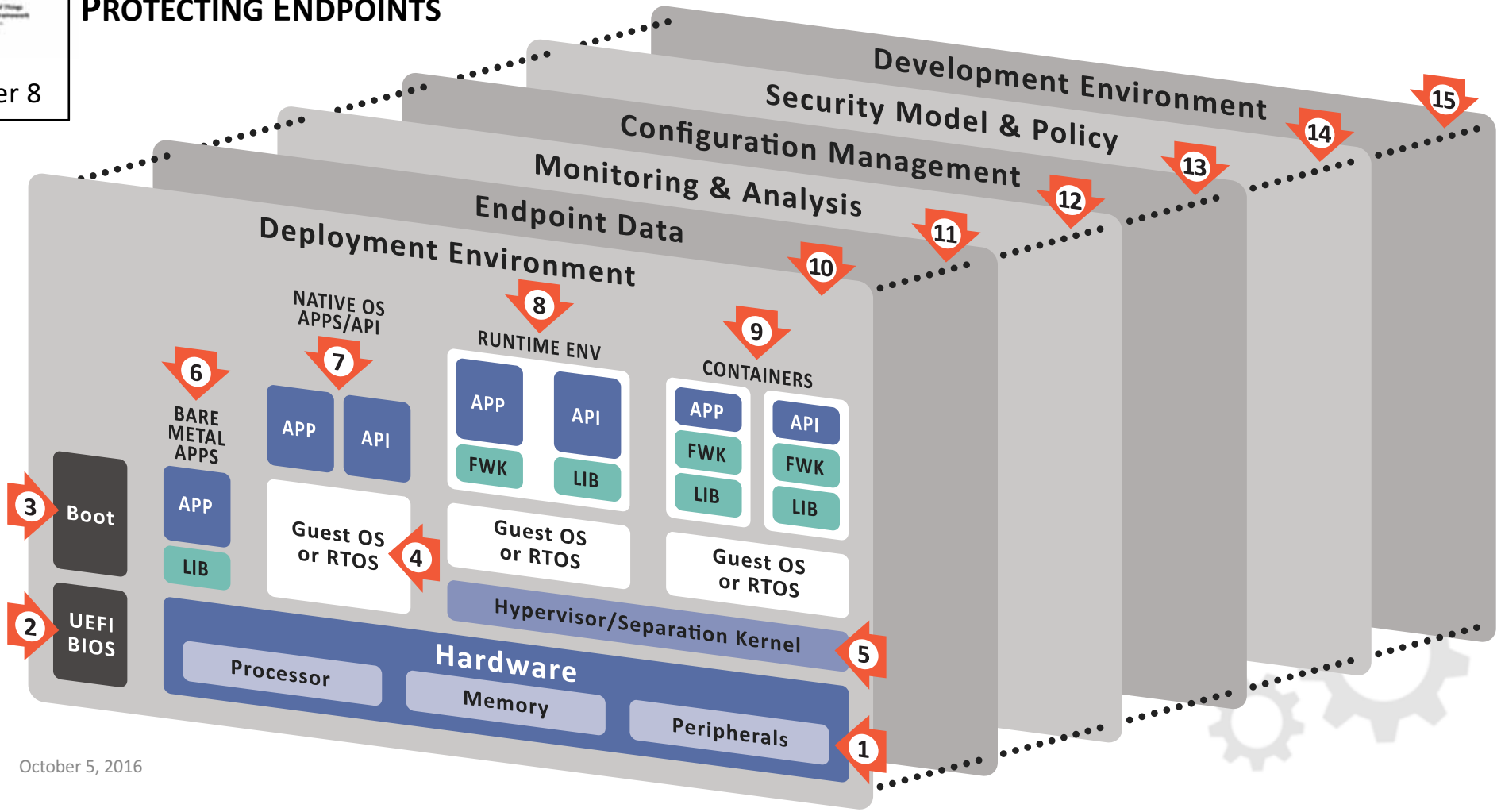
Chapter 7

Security Model & Policy
Configuration & Management Security Policy
Monitoring & Analysis Security Policy
Communications & Connectivity Security Policy
Endpoint Security Policy
Data Protection Security Policy
Security Policy
Security Model
System Security Objectives
System Threat Analysis

Chapter 8

PROTECTING ENDPOINTS

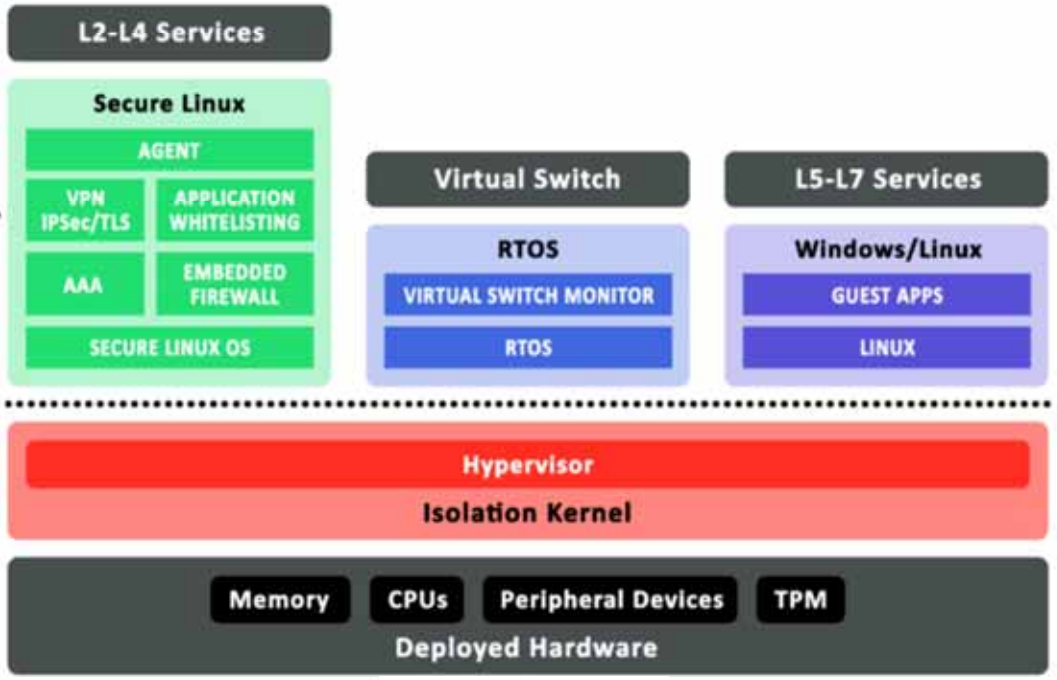
THREAT AND VULNERABILITIES TO IIOT ENDPOINTS



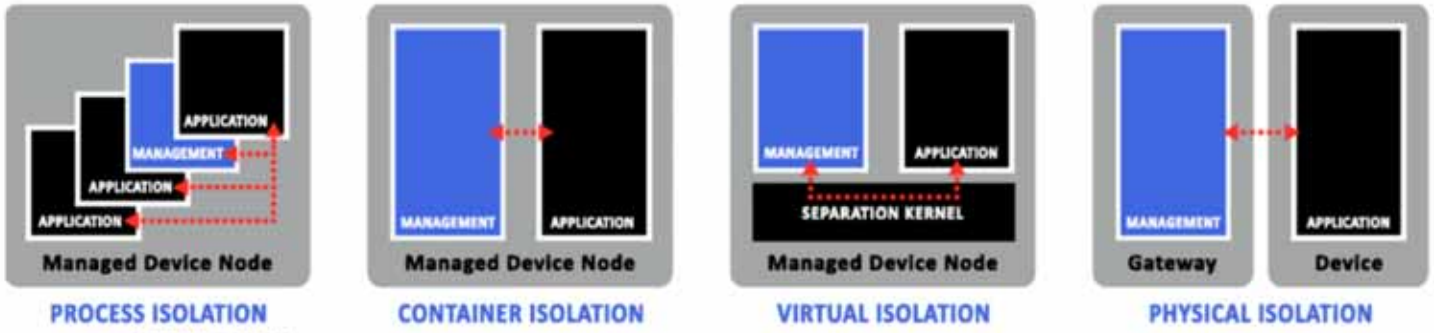
October 5, 2016

Chapter 8

PROTECTING ENDPOINTS



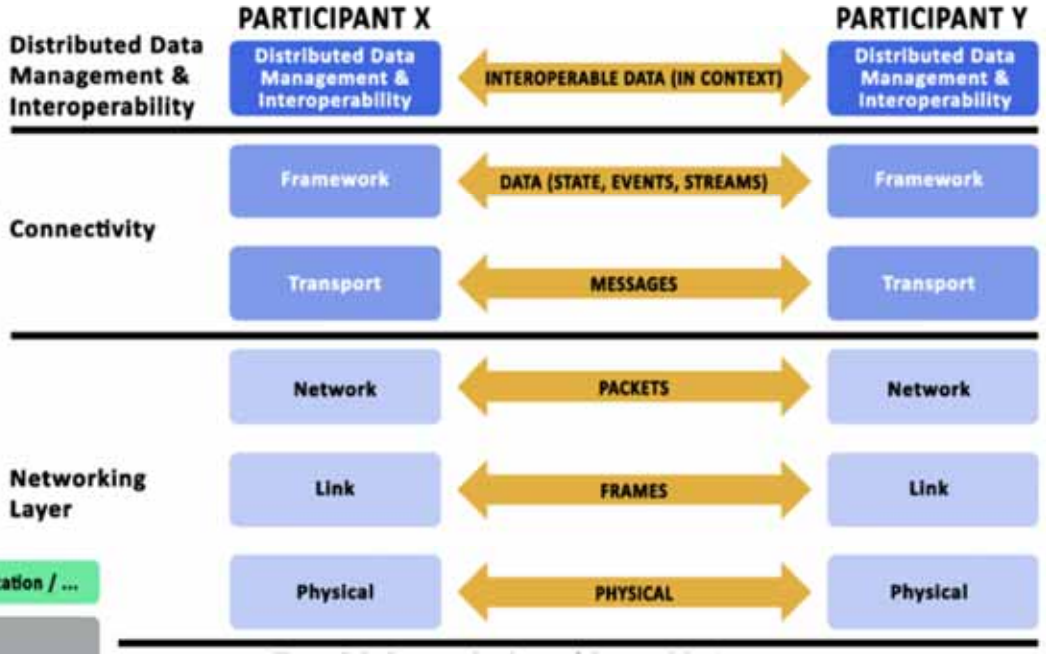
Virtual Isolation



Endpoint and Container Isolation Techniques

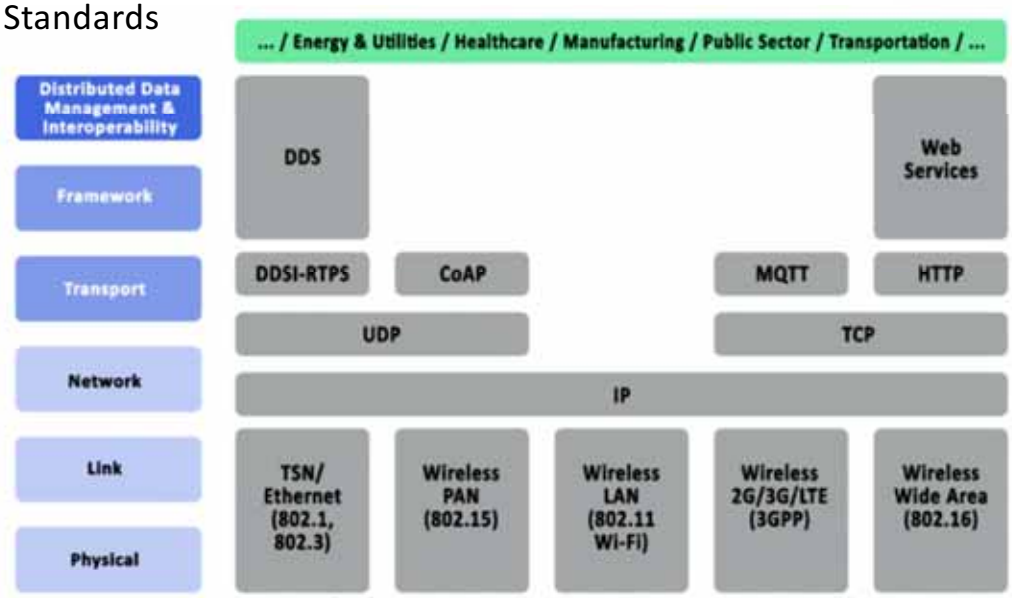
CHAPTER 9

PROTECTING COMMUNICATIONS AND CONNECTIVITY



Communication and Connectivity Layers

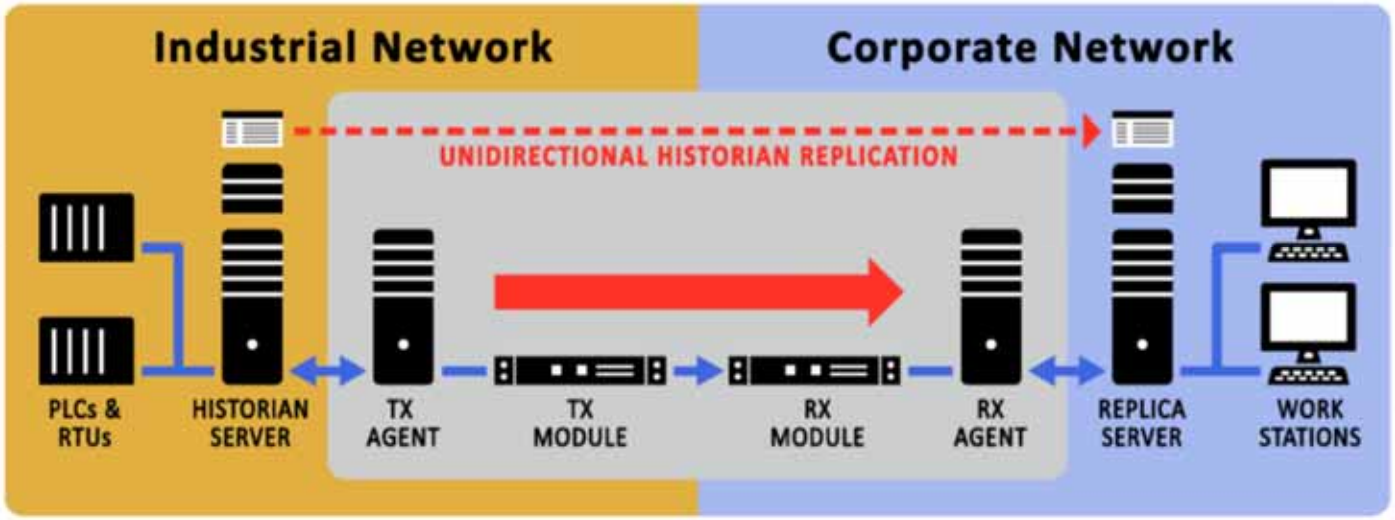
Example of IIoT core Communication & Connectivity Standards



CHAPTER 9

PROTECTING COMMUNICATIONS AND CONNECTIVITY

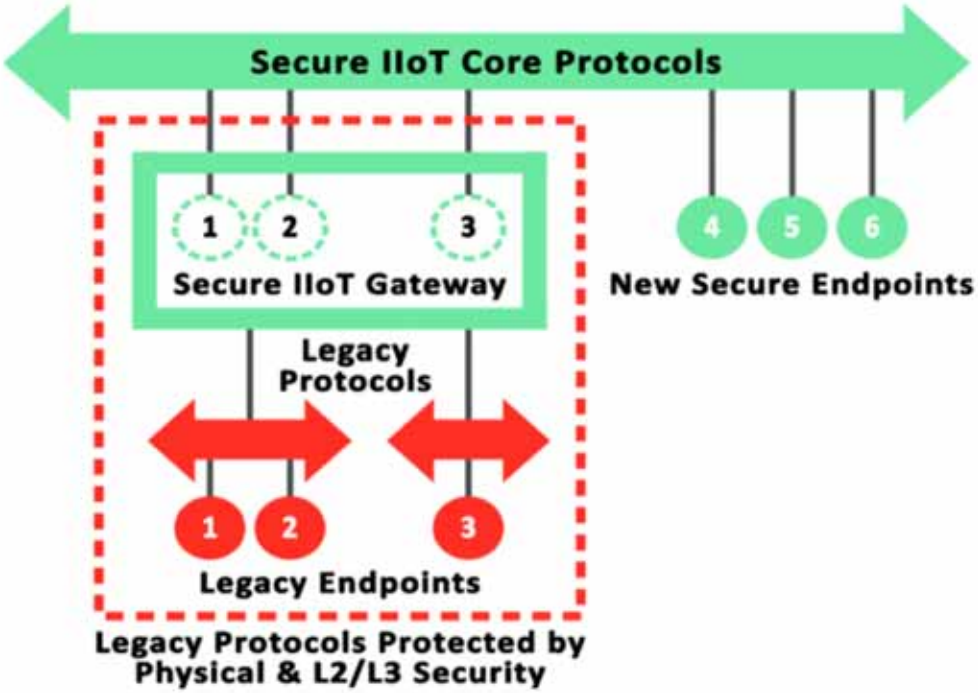
Communications Channels between IIoT Endpoints



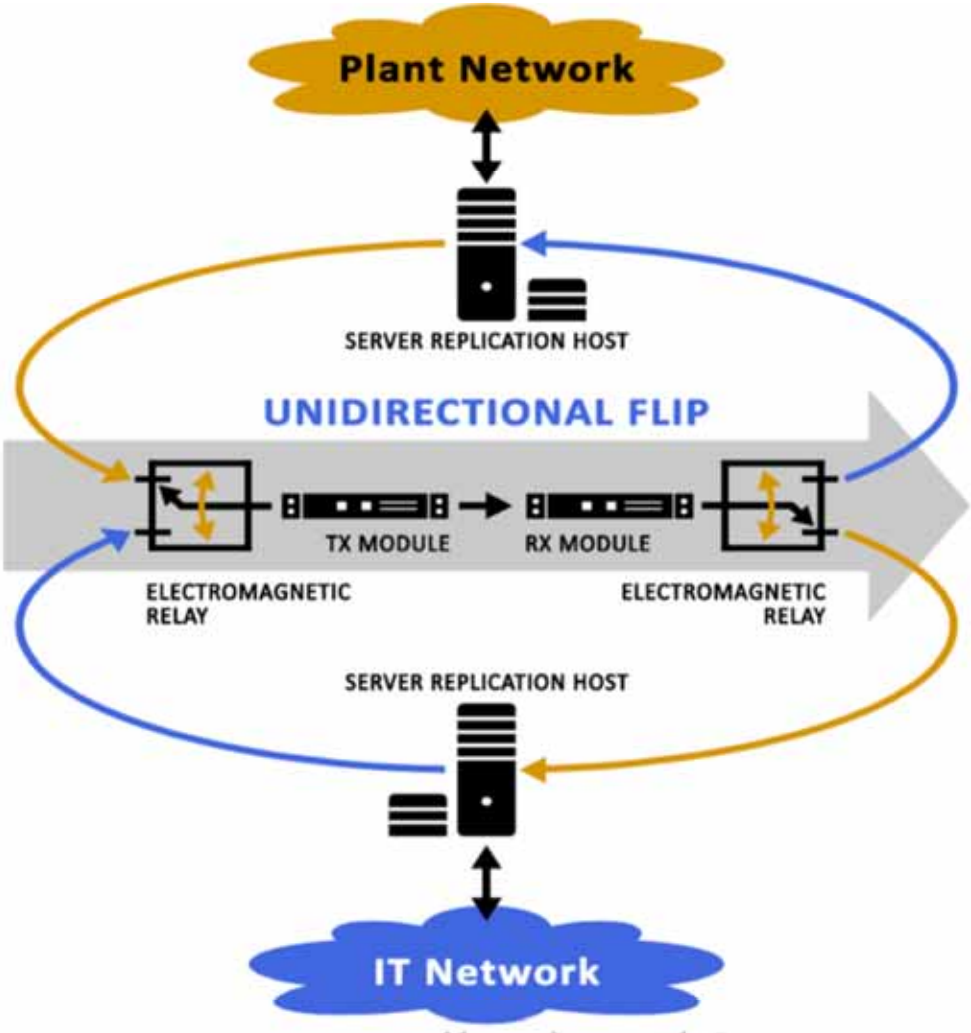
Unidirectional Plant Historian Replication

CHAPTER 9

PROTECTING COMMUNICATIONS AND CONNECTIVITY



Protecting Legacy Endpoints and Communication Links Using Gateways

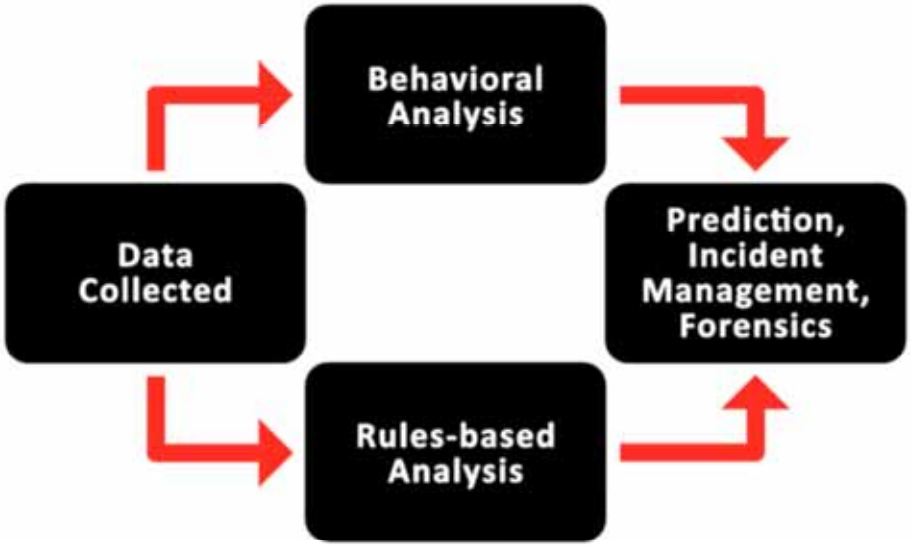


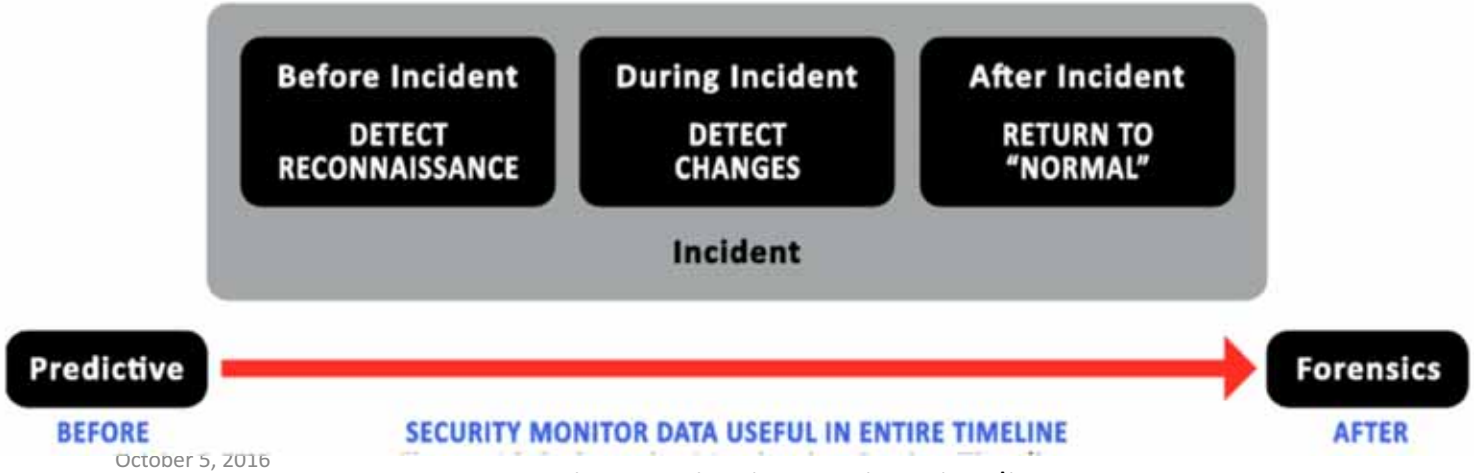
A Reversible Unidirectional Gateway

Chapter 10

SECURITY MONITORING AND ANALYSIS

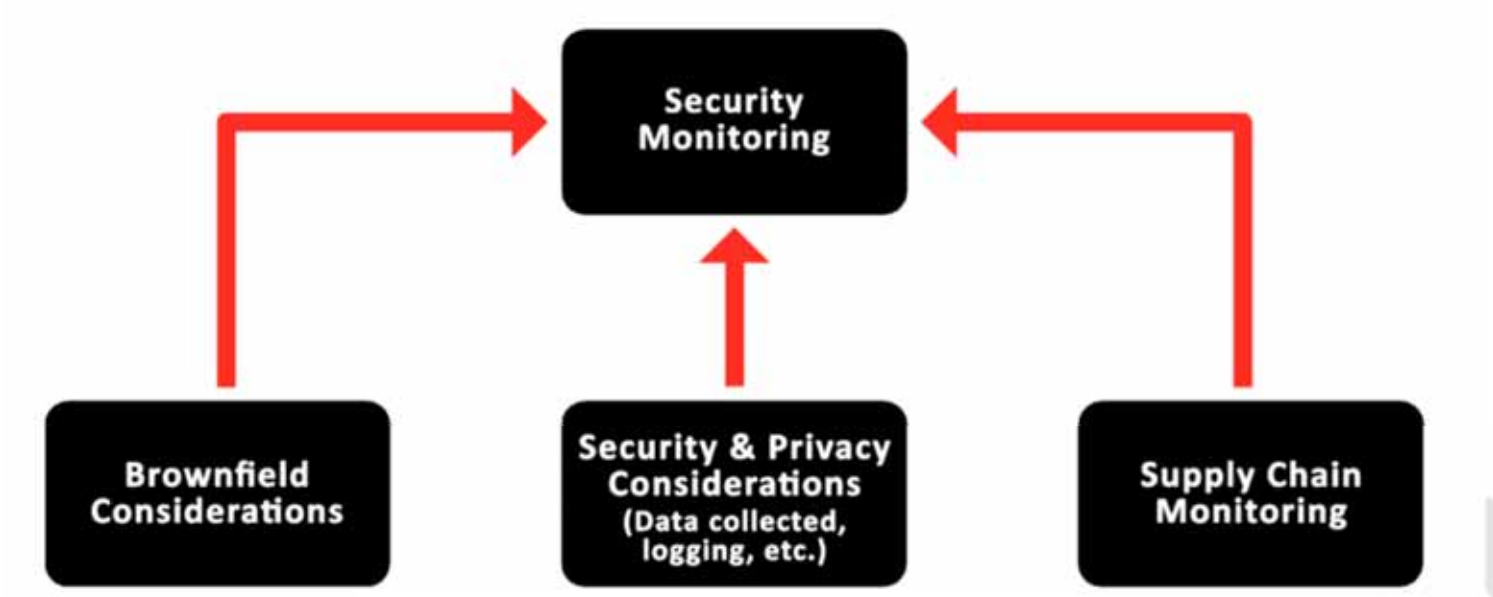
Security Monitoring Data Analysis Variants





Security Monitoring During Timeline

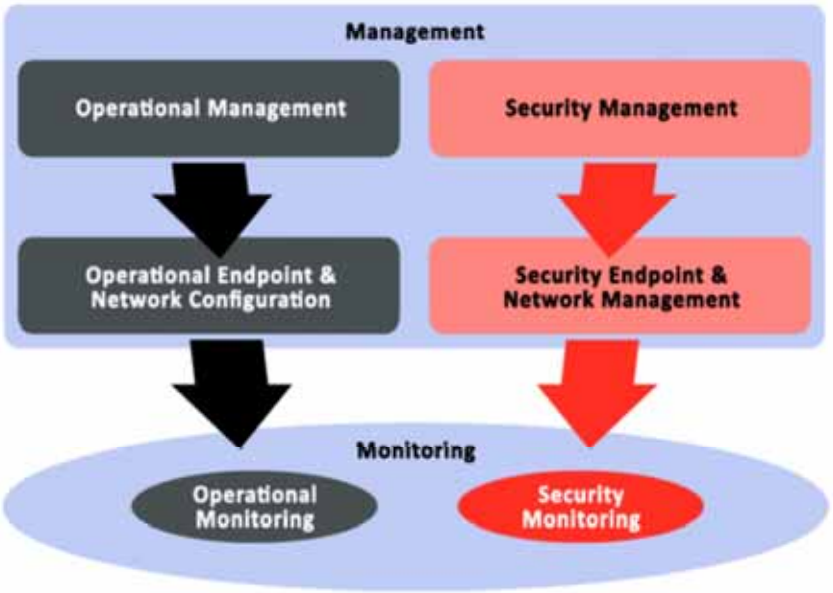
SECURITY MONITORING AND ANALYSIS



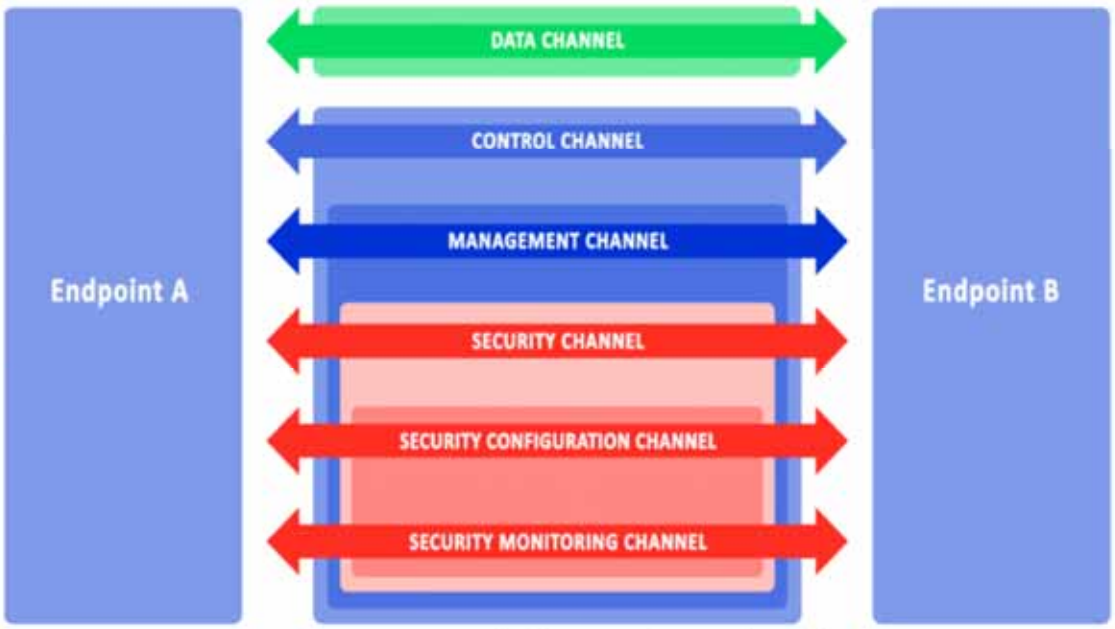
Security Monitoring Special Considerations

Chapter 11

SECURITY CONFIGURATION AND MANAGEMENT



Secure Operational Management

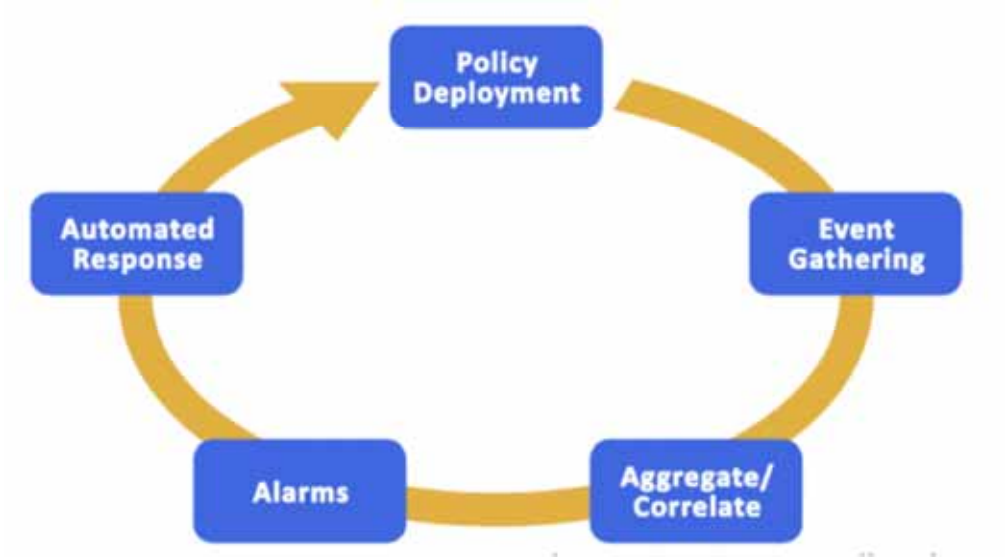


Hierarchical Communications Channels

Chapter 11

SECURITY CONFIGURATION AND MANAGEMENT

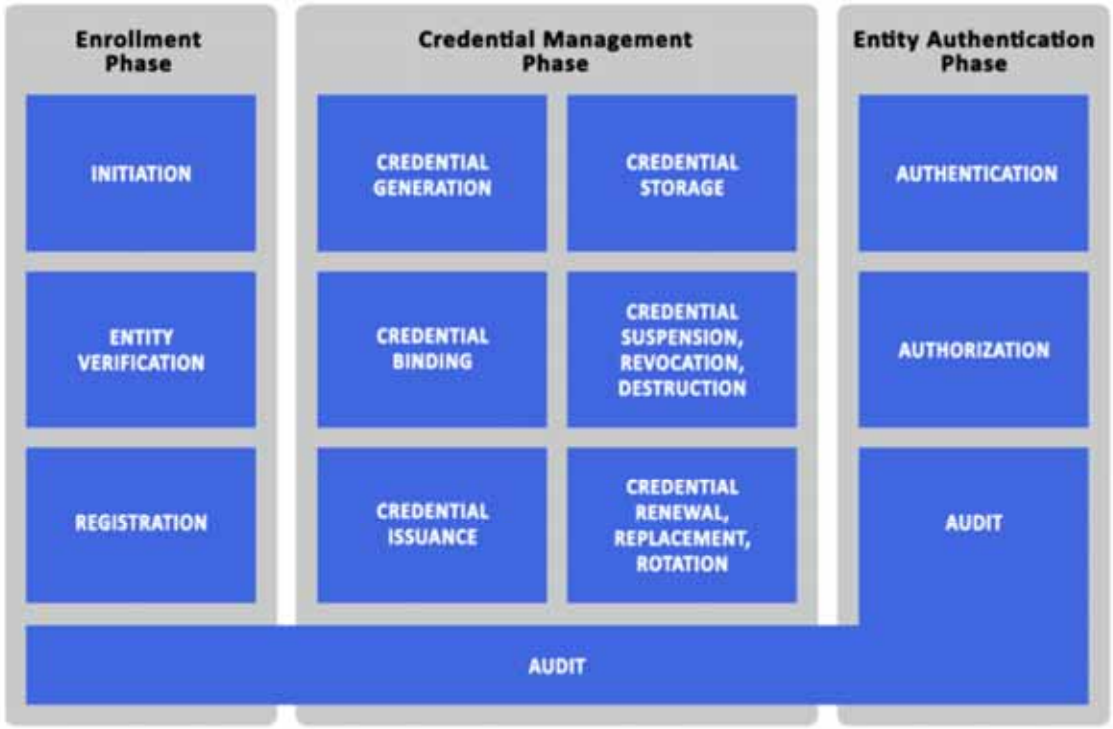
Policy Relationship



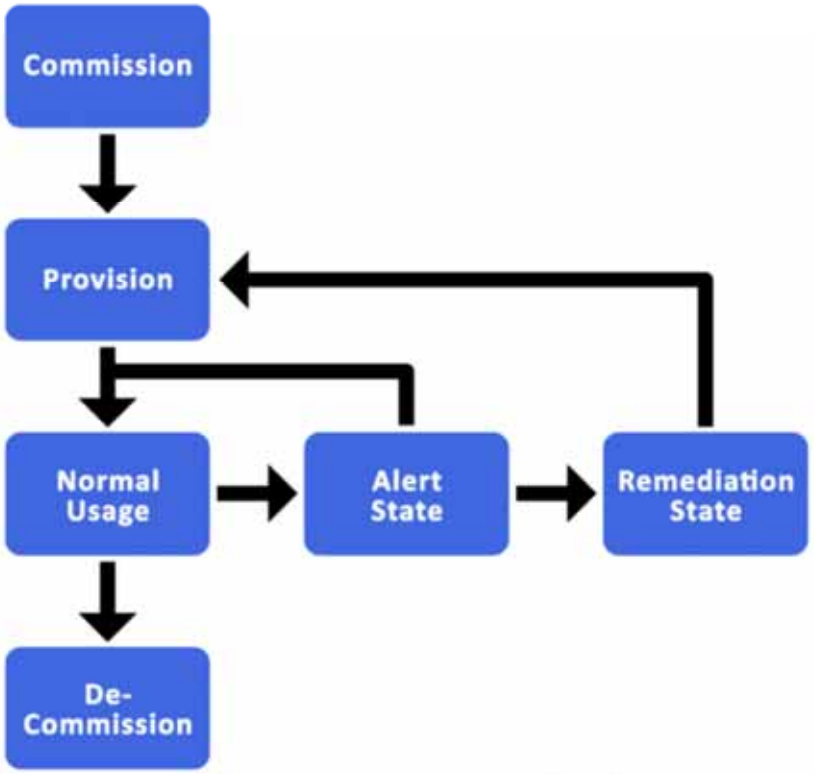
IIoT Management and Monitoring Feedback Loop

Chapter 11

SECURITY CONFIGURATION AND MANAGEMENT

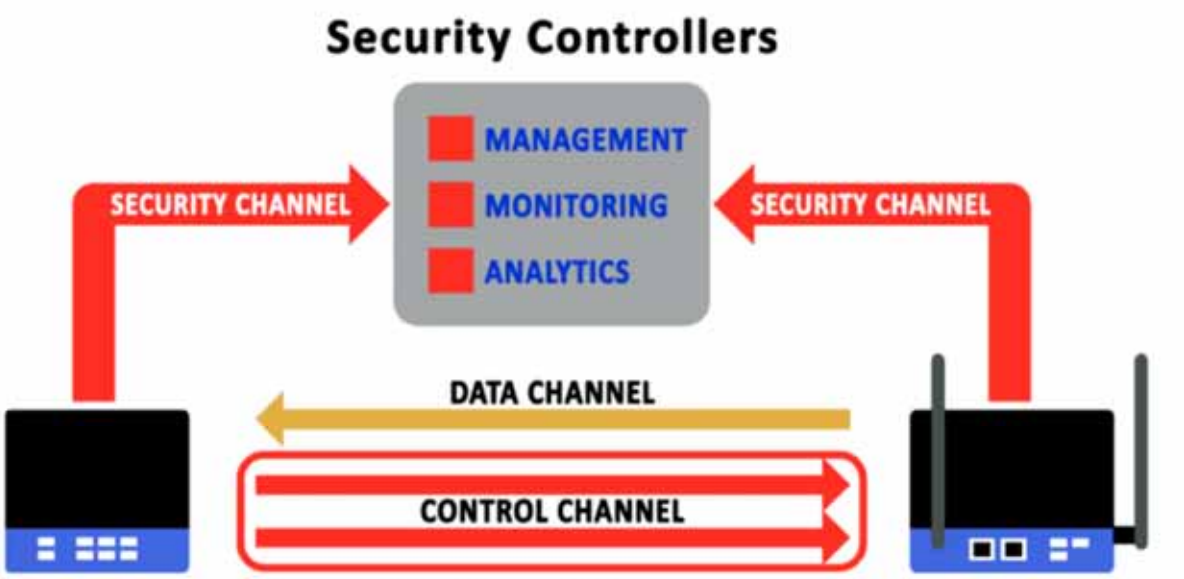


IIoT Identity Management Lifecycle



Endpoint Security Lifecycle

SECURITY CONFIGURATION AND MANAGEMENT



Flow of Management Data

Chapter 12 LOOKING AHEAD—THE FUTURE OF THE IIOT

mass customization

just-in-time manufacturing

software-defined network

homomorphic encryption

microelectromechanical system

desktop milling

blockchain

high-assurance microkernels

quantum computing

split key technology

microservice

software-defined platforms and virtual machines

horizontally scalable computing infrastructures

venture funding and crowd funding

battery-friendly wireless protocols

pipelined single-piece workflow

physical unclonable functions

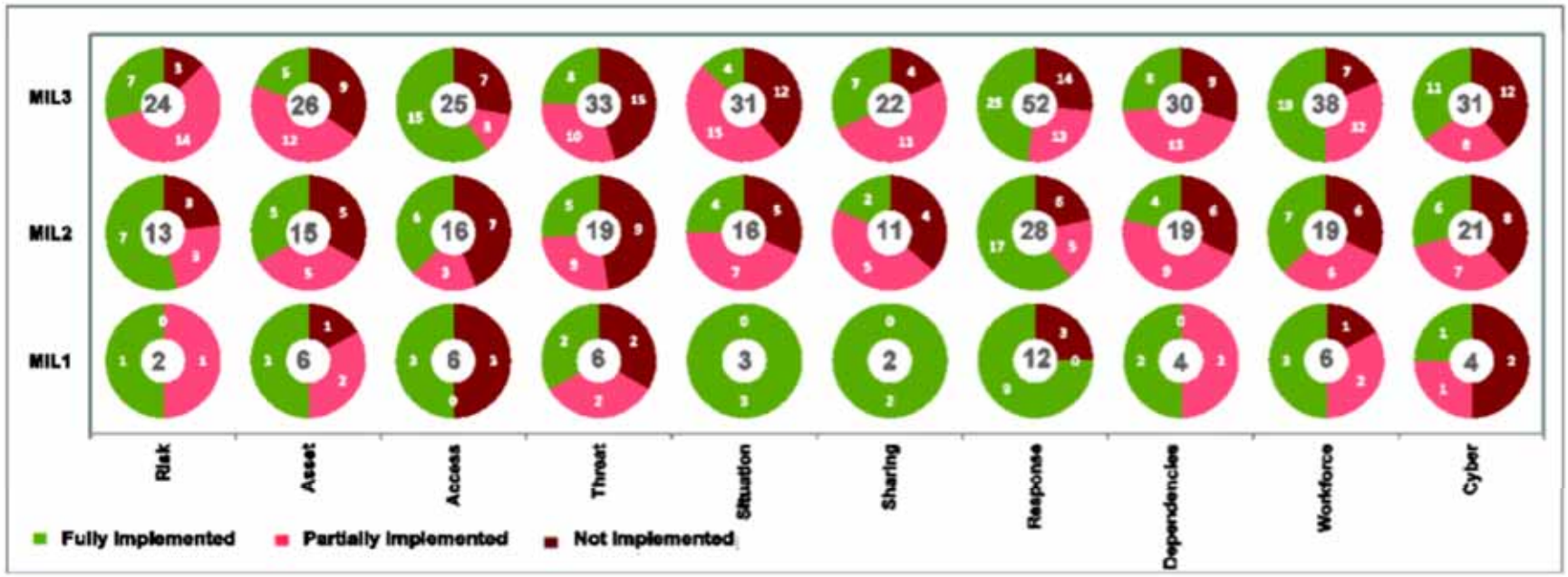
additive manufacturing

falling costs of bandwidth

intelligence at the edge

centralized to decentralized

Annex A: INDUSTRIAL SECURITY STANDARDS
Annex B: CYBER SECURITY CAPABILITY MATURITY MODEL (C2M2)



Annex C: SECURITY CAPABILITIES AND TECHNIQUES TABLES

Cryptographic Technique		Example Objective	Example Requirements	
Symmetric key cryptography	MACs	Message authentication; Message integrity	Securely generated, distributed and maintained, shared secret key	Secure standardized and up-to-date MAC algorithm
	Symmetric encryption	Confidentiality		Secure standardized and up-to-date encryption algorithm
Asymmetric key cryptography	Digital signatures	Authorship; Integrity; Non-repudiation	Public-key infrastructure	Standard-based securely generated, distributed and maintained, public and private keys; Standardized and up-to-date signature schemes
	Asymmetric encryption	Confidentiality		Standardized and up-to-date asymmetric encryption algorithm
	Shared secret establishment	Forward secrecy		Standardized and up-to-date shared secret establishment algorithm
Hash function		Message/data integrity		Standardized and up-to-date hashing algorithm
Random number generator		Random key and other data	Proper random seed	Standardized and up-to-date random generator

Cryptographic Techniques, their Objectives and Requirements

Annex C: SECURITY CAPABILITIES AND TECHNIQUES TABLES

Objective: Availability	Example Technique/Process	Example Requirements
Endpoint availability	Physical protective enclosure	Trusted manufacturing and deployment
Availability of communications	Physical availability of communications media; Network load management; Anti-jamming techniques	Trusted manufacturing and deployment
Availability of management and monitoring operations and solutions	Resource allocation; Planning for frequent iterative security evaluation	Evaluation methodology; Endpoint, communications and architectural availability for management and monitoring components
Architectural availability	Redundancy; Avoiding single points of failure; Fault tolerance; Load balancing; Honeypots	Architectural threat modeling

Techniques and Processes for Enabling System Availability

Techniques and Processes for Enabling System Integrity

Objective: Integrity		Example Technique/Process	Example Requirements
Endpoint integrity	Integrity for roots of trust	Protected key store	Integrity of protected storage for key management
	Integrity of endpoint identity	Identity certificate signed by trusted certificate authority	Trusted public-key infrastructure
	Hardware integrity	Side channel measurements; silicon scanning	Open, standards-based specification
	Software integrity	Code signing	Trusted public-key infrastructure
		Secure software development; Risk-based security testing; Static analysis	Secure software development methodology
		Boot process integrity	Trusted hardware manufacturer; Hardware security module or proprietary implementation of hardware backed cryptographic boot protection; Standardized OS firmware interface (e.g. UEFI)
		Secure patch management	Patch management plan
	Runtime integrity	Runtime verification	Code execution modeling, instrumentation and monitoring
	Integrity of data-at-rest	MACs, hashes/digests; Digital Signatures	Securely generated, distributed and maintained keys; Standardized and up-to-date algorithms
Integrity of communications		Mutual authentication between endpoints; use of MACs and/or digital signatures during communication	Securely generated, distributed and maintained keys; Standardized and up-to-date algorithms for mutual authentication and message exchange integrity
Integrity of management and monitoring operations		Authentication of management and monitoring assets (including workforce); Integrity verification of asset changes, asset monitoring solutions and asset Updates; Maintaining integrity of logs and reports	Endpoint integrity for management and monitoring; Communication integrity for monitoring, logging and management of assets; Security procedures for managing management and monitoring operations; Integrity of analytical algorithms; Integrity of audit or audit path
Architectural integrity	Integrity of data-in-motion	Holistic assessment of data integrity in its lifecycle across the entire IIoT system	Endpoint, communication, monitoring and management integrity in system segments
	Mutual impact of integrity controls on other key system characteristics	Architectural integrity evaluation	Holistic security evaluation methodology; Domain-specific expertise
	Mitigating impact of both insider and outsider attacks on system integrity	Enforcing principle of least privilege; Access control	Granular access control policies

Annex C: SECURITY CAPABILITIES AND TECHNIQUES TABLES

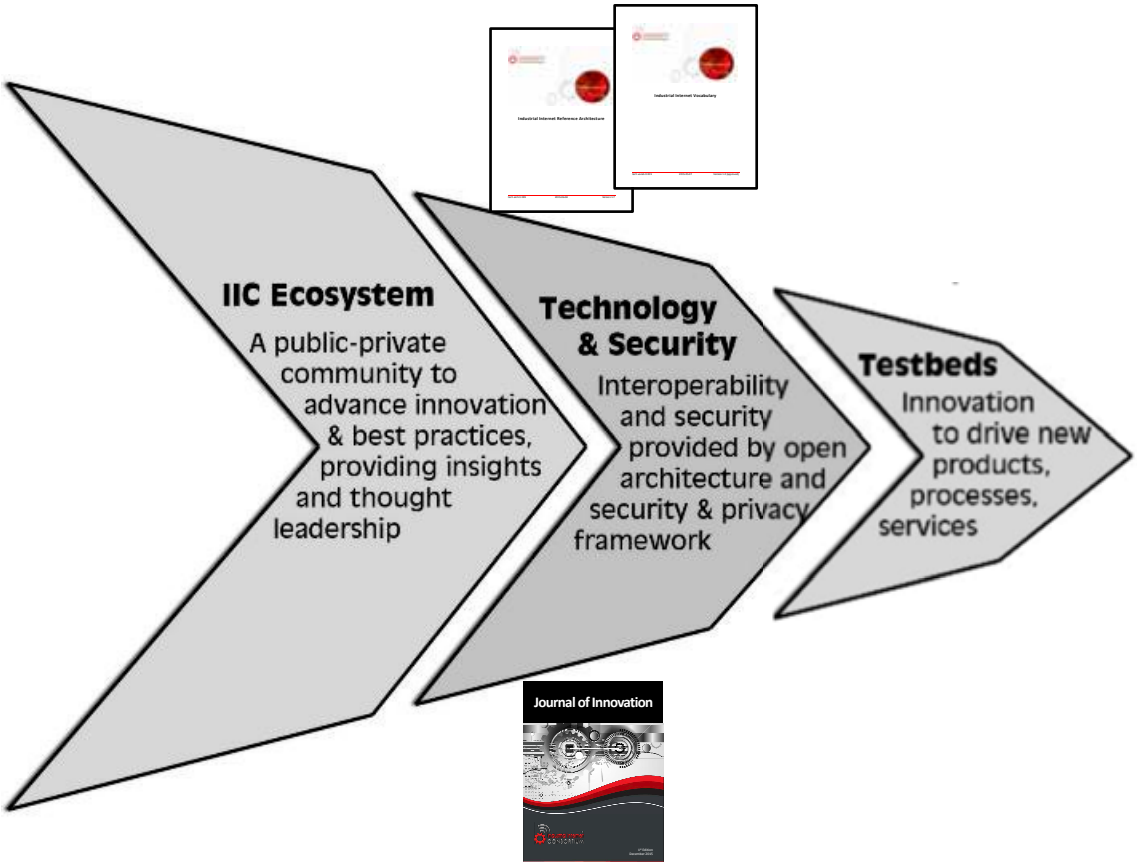
Objective: Confidentiality		Example Technique/Process	Example Requirements
Confidentiality at endpoints		Encrypted data storage	Securely generated, distributed, and maintained keys; Protective storage of sensitive key material; Standardized and up-to-date encryption algorithms
Confidentiality of communication		Encrypted communication	Securely generated, distributed, and maintained keys; Standardized and up-to-date encryption algorithms
Confidentiality of management and monitoring operations and solutions		Encrypted communication	Endpoint confidentiality and communications confidentiality
Architectural confidentiality	Confidentiality of data in its lifecycle		Endpoint confidentiality; communications confidentiality; Confidentiality of management and monitoring
	Mutual impact of confidentiality controls on other key system characteristics	Architectural confidentiality evaluation	Holistic security evaluation methodology; Domain-specific expertise
	Mitigating impact of both insider and outsider attacks on confidentiality	Enforcing principle of least privilege; Access control	Granular access control policies

Techniques and Processes for Enabling System Confidentiality

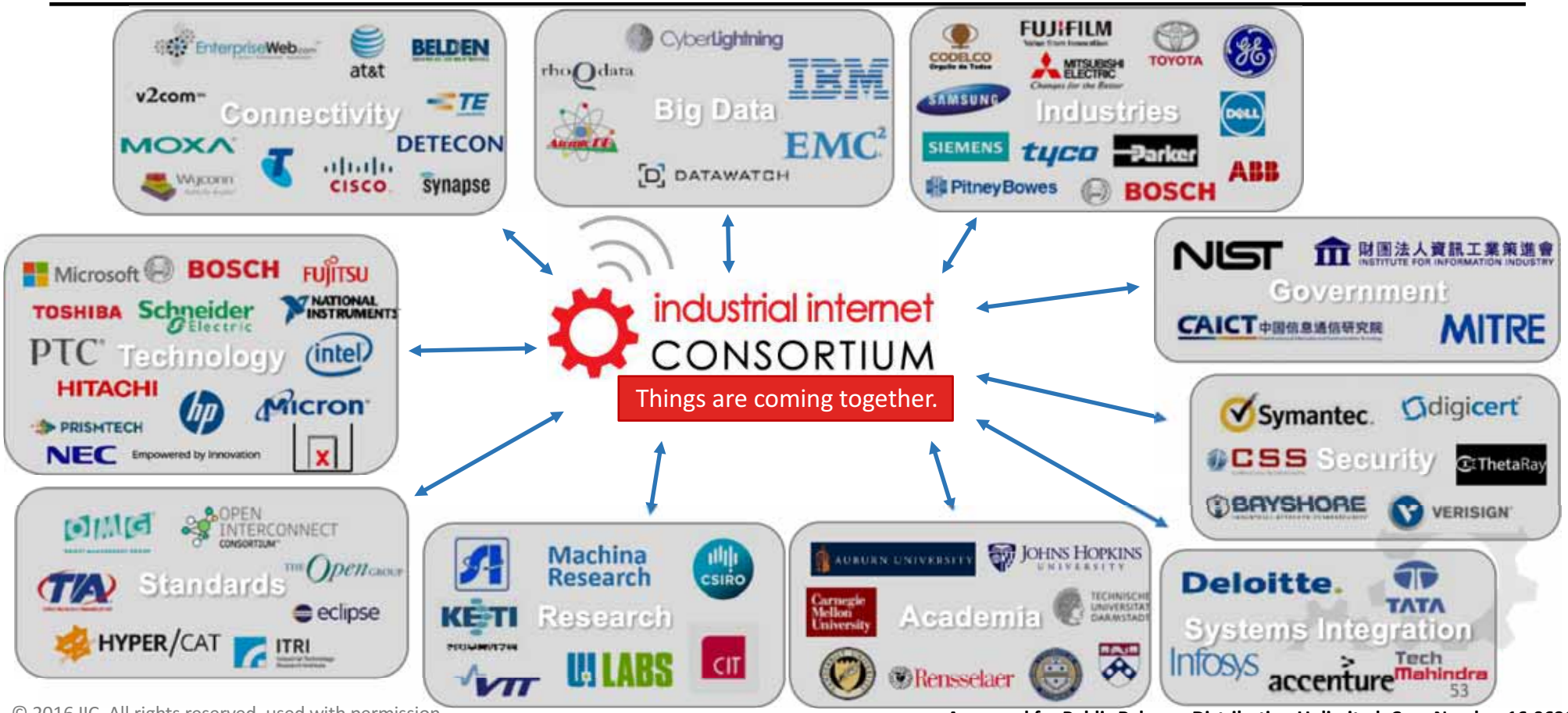
Techniques and Processes for Enabling System Access Control

Objective: Access Control		Example Technique/Process	Example Requirements
Endpoint access control	Confinement and information flow protection within endpoint	Sandboxing (application); Fine-grained data-centric access control (middleware); Separation kernels (OS); Trusted computing environments (hardware)	Comprehensive and consistent security policies
Communications access control	Cryptographic protection of communications and connectivity	Use of protocols at different layers; Forcible disconnection of unauthorized endpoints;	Correct and trusted implementation of cryptographic techniques; Network access control for endpoints
	Information flow control	Network segmentation; Gateways and filtering; Network firewalls; Unidirectional gateways	Comprehensive and consistent security policies; Trusted manufacturing of devices
Access control for management and monitoring operations			Access control for monitoring, logging and managing assets (e.g. endpoints, communication, data, workforce); Control procedures for managing and monitoring operations; Controlling access to data that is fed into analytics solutions; Separation of duties; Role-based access control (RBAC)
Architectural access control	Controlling access to data in its lifecycle		Access control within endpoints, communication, management and monitoring
	Mutual impact of access controls on other key system characteristics	Architectural access control evaluation	Holistic security evaluation methodology; Domain-specific expertise
	Mitigating impact of both insider and outsider attacks on access control	Enforcing principle of least privilege	Granular access control policies

The IIC has three primary areas of activity: Community Engagement, Technology & Security, and Testbeds



The IIC: Things are coming together



The End

<ramartin@mitre.org>

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.